Optimization of Symmetric Key Management in Wireless Mesh Networks

Project Report Submitted in partial fulfillment of the requirement for the degree of

Master of Technology

in

Computer Science & Engineering

under the Supervision of

Dr. Hemraj Saini

By

Aashish Rao(132215)

Jaypee University of Information Technology
Waknaghat, Solan – 173234, Himachal Pradesh
May 2015

Certificate

This is to certify that project report entitled **"Optimization of Symmetric Key Management in Wireless Mesh Networks"**, submitted by **Aashish Rao** in partial fulfillment for the award of degree of Master of Technology in Computer Science & Engineering to Jaypee University of Information Technology, Waknaghat, Solan has been carried out under my supervision. This work has not been submitted partially or fully to any other University or Institute for the award of this or any other degree or diploma.

Supervisor's Name:

Dr. Hemraj Saini

Date:

Designation:

Assistant Professor(CSE)

(Senior Grade)

Acknowledgement

First of all, I am very thankful to Almighty God for granting me the wisdom, health and strength for doing this work. Next, I am thankful to my supervisor **Dr. Hemraj Saini** for providing me an opportunity to work under him. I am indebted to him for being a constant source of knowledge for me from taking of this thesis till now. He not only corrected me in the technical issues related to the my thesis work, but his painstakingly report correction as well as presentation helped me a lot to represent this research work in a novel way.

I owe a deep gratitude to **Dr. Vivek Sehgal**, **Dr. Yashwant Singh**, **Dr. Shailendra Shukla**, **Mr. Amol Vasudeva**, and **Mr. Ravindra Bhatt** for not only being the panel members of my thesis report evaluation, but also providing insightful comments at different times during this semester.

At last, I would like to say that all this would have been difficult to achieve without the support and patience of my parents. They have been a source of consistent motivation for this work. I love them for their perseverance and the moral character they provided to me.

Name of the student:
Date:
Aashish Rao

CONTENTS

LIST OF FIGURES

ABBREVIATIONS

WMNs	**W**ireless **M**esh **N**etworks
WSN	**W**ireless **S**ensor **N**etworks
MRs	**M**esh **R**outers
MCs	**M**esh **C**lients
MANETs	**M**obile **A**d **H**oc **N**etworks
PKI	**P**ublic **K**ey **I**nfrastructure
ISP	**I**nternet **S**ervice **P**rovider
WLAN	**W**ireless **L**ocal **A**rea **N**networks
VOIP	**V** **O**ver **IP**
PKC	**P**ublic **K**ey **C**ryptography
TTP	**T**rusted **T**hird **p**arty
AES	**A**dvance **E**ncryption **S**standard
DES	**D**ata **E**ncryption **S**standard
3DES	**T**riple **D**ata **E**ncryption **S**standard
CA	**C**ertification **A**uthority
IBE	**I**dentity **B**ased **E**ncyption
PKG	**P**rivate **K**ey **G**enerator
OKM	**O**ptimized **K**ey **M**anagement

Abstract

Wireless mesh networks (WMNs) provide us different kind of technology foraccessing broadband network. Advantageous to clients by providing universal access to avail internet services and to service providers by providing low deployment cost for setting up the infrastructure.Lack of security inWMNs architecture and its vulnerability to malicious attacks due to the nature of wireless communication is hindering the large scale deployment of WMNs. While a lot of effort has been done in securing the wireless sensor networks (WSNs) and MANETs, WMNs are still not fully explored with respect to securing the network involving the symmetric keys. Integration of various kind of networks, need for multi–hop wireless communication and absence of centralized trusted authority are the endless demands of WMNs, due to which the conventional security mechanisms have become incompetent. WMNs requires lightweight key management schemes, instead of public key infrastructure (PKI) as it demands no limitations on the available resources. In this work while considering these facts the architecture we considered is made more robust and secure by deploying the PKI along with symmetric key management; initial key exchange is being carried out in asymmetric manner while key distribution and key management after initial key exchange is being carried out in a symmetric way. The proposed architecture includes a trusted third party for securing the network and makes it scalable. Additionally it also minimizes the communication and storage overhead.After the experiment and simulation, the results obtained after considering the architecture we proposed are effective for enhancing the security of WMNs.

CHAPTER 1

INTRODUCTION

1.1 Overview

The Wireless Mesh Network is an emerging technology the inexpensive network deployment, high speed and easy internet connectivity features makes it a popular choice for Wireless ISP (Internet Service Provider). Wireless Mesh Networks (WMNs) involve mesh routers and mesh clients, where mesh routers have nominal mobility and form the pillars of WMNs. Some of mesh routers functions as gateways. The mesh clients are frequently laptops, cell phones and other wireless devices however the mesh routers forwards data to and from the gateways which may, but need not, join to the Internet. WMN is responsible for providing network access for both mesh and conventional clients. The integration of WMNs with other networks such as internet, cellular networks, sensor networks etc., can be attained through the gateway and bridging functionality of MRs.

Wireless mesh architecture is the primary step towards providing cost effective and dynamic high-bandwidth networks over a specific coverage zone. Wireless mesh architectures infrastructure is, in effect, a router network minus the cabling between nodes. It's built of peer radio devices that don't have to be cabled to a wired port like traditional WLAN access points do. Mesh architecture sustains signal strength by breaking long distances into a series of shorter hops. Intermediate nodes not only boost the signal, but cooperatively make forwarding decisions based on their knowledge of the network, i.e. perform routing. Such architecture may with careful design provide high bandwidth, spectral efficiency, and economic advantage over the coverage area.

As the size of a wireless mesh network increases, the number of Internet connected access points (Internet gateways) needs to increase to disperse traffic and avoid congestion. In practice, Internet gateways will reside at different locations and will often be connected to different network domains In this type of networks, a mobile client is served by a nearby access point that forwards data packets (potentially over multiple wireless hops) to its closest Internet gateway.

The WMN is relevant in various scenarios such as disaster situations, tunnels, oil rigs, battlefield surveillance and high speed mobile video applications on board public transport or real time racing car telemetry. A significant potential application for WMNs is VoIP. By using a Quality of Service scheme, the wireless mesh supports local telephone calls to be directed through the mesh.

Symmetric key management comprises of a single, common key that is used to encrypt and decrypt the information exchanged among users. A trusted party provides each applicant a secret key and a public identifier, which enables any two participants to independently create a shared key for communication. Contrast this with public key cryptology, in Asymmetric cryptography we use two keys i.e. private keys which is known by the node itself and public key which is known by other nodes. Here total keys is to be known by a node is reduced to n. As far as security and computation is concerned we get attracted toward public key cryptography [2] .There are numerous PKC techniques has been evolved like RSA, diffie Hellman , elliptic curve cryptography etc., but in our proposed approach we are focusing on identity based cryptography.

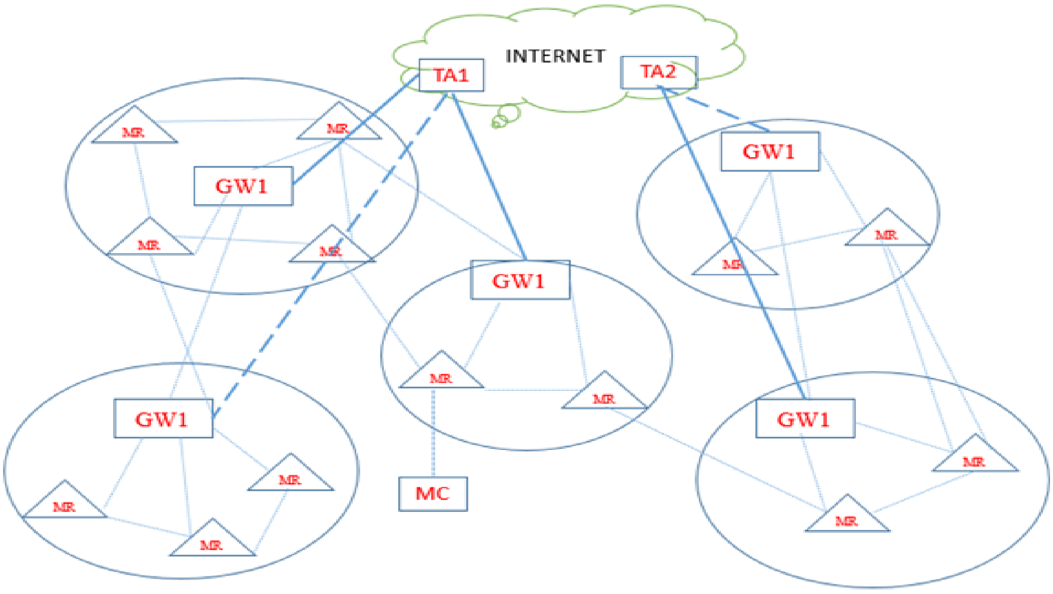


FIGURE 1.1: Architecture of wireless mesh network (adapted from [1])

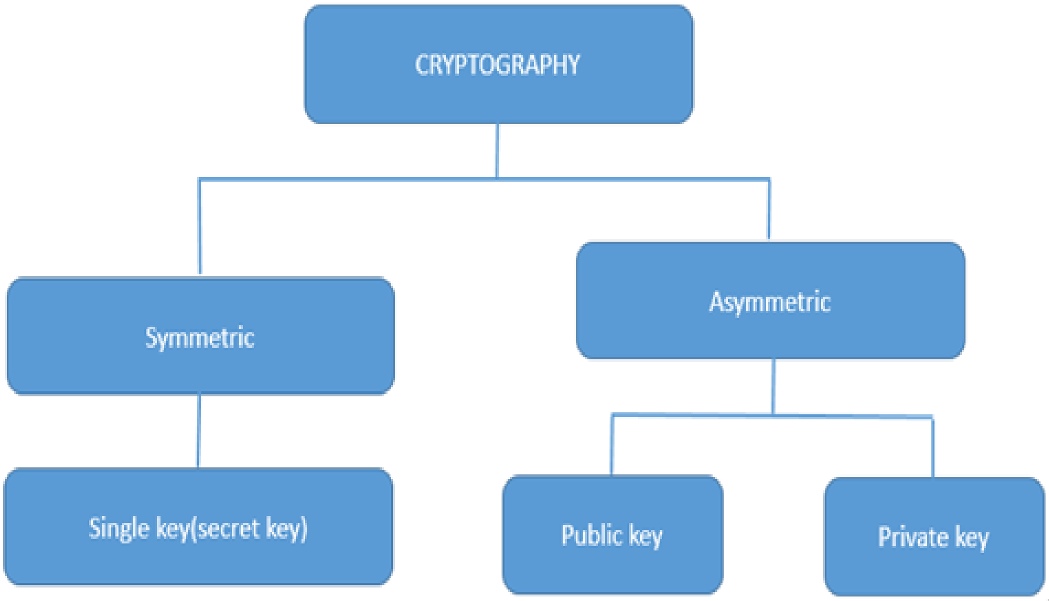


FIGURE 1.2: Cryptography Taxonomy

The Wireless Mesh Network is an emerging technology, its fast, inexpensive network deployment, easy internet connectivity features makes it a popular choice for Wireless ISP (Internet Service Provider). WMN represents the combination of Wide area cellular network and high speed Wi-Fi networks. Nevertheless, without any security in WMN, it is impossible to securely exchange any information. [2-9]. various research works is in progress. At present there are no formal methods to authenticate the network in WMN. Security is an open challenge in WMN. In recent times lot of research work is in progress. (Fu.et.al)[10] Proposed an authentication scheme in which he integrate various existing techniques i.e. Virtual certificate authority, zone based hierarchical structure and multi signature scheme. (Zhang et.al) [11] Proposed architecture, in which, if mesh client wishes to roam to another network, then it require a pass from trusted third party. In his another work he proposed a scheme in which matrix based pairwise key establishment is being enhanced by deploying some pre deployment knowledge.

1.2 Symmetric-key Cryptography and AES

Symmetric-key cryptography, also known as secret key cryptography, is the most perceptive kind of cryptography. It is based on the use of a secret key recognized by nodes which are involved in secure communication. Symmetric-key cryptography can be used to exchange secret data on an insecure channel, but it also services such as protected storage on vulnerable media or physically powerful mutual authentication. The concept in symmetric-key cryptography is to distribute the key among sender and the receiver. The sender then encrypts the data using the key and encryption function to produce the ciphertext. The receiver receives the ciphertext, who then applies the decryption function using the same shared key. While the plaintext cannot be derived from the ciphertext without prior information of the key, hence ciphertext can be sent over public networks. Consequently, symmetric key cryptography is characterized by the bringing into play of a single key for encryption and decryption. . If key is preserved, both the secrecy and authentication services are offered. Secrecy in the network is offered, because if the message is interrupted, the intruder cannot alter the ciphertext into its plaintext format. Supposing that only two users know the key, authentication is provided because only a user with the key can generate ciphertext that a recipient can modify into significant plaintext. The standard used in United States of America for Symmetric-key cryptography, in which the same key is used for both encryption and decryption, is the **Data Encryption Standard (DES)** [36]. DES works over a combination and permutation of shifts and exclusive OR operations and so can be very firm when applied straightly on hardware (1 GByte/s throughput or better) or on general purpose processors. DES utilizes a 56-bit key and plots a 64-bit input data block of plaintext onto a 64-bit output data block of ciphertext. Considering the 56-bit key in current period cannot be considered strong key. The majority cryptographic community has withdrawn its hand from DES. As 56-bit key is very short to survive a brute-force attack from recent computers. Computers have made it easier to outbreak ciphertext by using brute force methods instead of attacking the mathematics. Considering brute force attack, the enemy does not produces every possible key and applies it to the ciphertext. Any subsequent plaintext that makes sense offers a applicant for a genuine key. The current key size of 56 bits (plus 8 parity bits) of DES is now starting to seem small, but the use of larger keys with triple DES (3DES) can make the network more secure. If we are only thoughtful about security, then 3DES will be a suitable choice for a standardized encryption algorithm for very long time. Nonetheless, the major drawback with 3DES is that the algorithm is moderately slow in software. Another disadvantage is the use of 64-bit data block, which is relatively small compared to modern period.

Due to above mention reasons DES is discarded and as a replacement, NIST (National Institute of Standards and Technology) of USA in 1997 gave out a call for proposals of a new **Advanced Encryption Standard (AES)**, which would have security length equal to or better than 3DES and considerably, enhances the efficiency. In accumulation to these universal requirements, NIST indicated that AES should be a symmetric block cipher with a fixed block length of 128 bits and support three different types of keys of lengths 128, 192, and 256 bits. The AES algorithm was adopted in October 2001 after a multi-year assessment process managed by NIST. Invented by Joan Daemen and Vincent Rijmen, was selected as the standard which was issued in November 2002. NIST's idealized to have a cipher that will persist secure well into the next century.

1.3 Aims of the Thesis

The main aims of this thesis is to provide a lightweight key management technique which is suitable for wireless mesh networks and is able to enhance its security while making the network scalable and distributing the load in the network, and to implement the protocol and find out its performance in respect to the space required to store the keys and time required in computation of the key distribution and show how the proposed scheme is suitable for wireless mesh networks.

1.4 Layout of the Thesis

This thesis is divided into seven major parts. This chapter introduces the basic overview of wireless mesh networks and the key management protocol along with aims of the thesis. **Chapter 2** gives a brief introduction about what work has been carried out in the literature and what current practices is being carried out related to key management in WMNs **Chapter 3** describes the services presented by the key management and challenges offered by key management in WMNs **Chapter 4** discusses the background knowledge required for carrying out any further work **Chapter 5** introduces the proposed key management for securing the WMNs

Chapter 6 contains the implementation and the results of our proposed approach, and **chapter 7** concludes our work along with the scope for future work.

CHAPTER 2

LITERATURE REVIEW

A WMN is dynamically self-organized and self-configured, with the nodes in the network automatically establishing and maintaining mesh connectivity among themselves (creating, in effect, an ad hoc network). Wireless mesh networks (WMNs) consist of mesh routers and mesh clients, where mesh router have minimum mobility and form the backbone of WMNs, while mesh clients are stationary or mobile and can form client mesh network among them and with mesh router.

The integration of WMNs with other networks such as the Internet, cellular, IEEE 802.11, IEEE 802.15, IEEE 802.16, sensor networks, etc., can be accomplished through the gateway and bridging functions in the mesh routers.

2.1 Network architecture

WMN architecture can be broadly classified into three kinds.

1. Infrastructure WMN's. This type of WMNs includes mesh routers forming an infrastructure for clients that connect to them.

2. Client WMN's Client meshing provides peer-to-peer networks among client devices.

3. Hybrid WMN's. This architecture is combination of infrastructure and client WMN.

2.2 Characteristics of WMN

1. Multihop wireless network, which makes the network scalable without sacrificing channel capacity.

2. WMN supports ad-hoc networking and has the capability of self-forming, self-healing and self organizing.

3. WMN supports various kinds of network access which are backhaul access to internet, peerto peer and integration of WMN with other kind of wireless device.

2.3 Applications of WMN

1. **Broadband home networking**

   Presently broadband home networking is realized through IEEE 802.11 WLANs. An observable problem is the position of the access points. Without a site survey, a home typically has many dead zones inside it. Solutions based on site survey are pricey and not convenient for home networking, while installation of multiple access points is also expensive and not convenient because of Ethernet wiring from access points to backhaul network access modem or hub. Likewise, communications between any two end nodes under two different access points have to go all the way back to the access hub. This is evidently not an proficient solution, especially for broadband networking. Mesh networking can determine all these issues in home networking and provide a solution for it. The access points in WLANs must be replaced by wireless mesh routers with mesh connectivity established amid them. Consequently, the communication among these nodes becomes much more flexible and more robust to network faults and link failures. Solution for elimination of dead zones is to raise the number of mesh routers in tha area., changing locations of mesh routers, and automatically adjusting power levels of mesh routers are some other solutions amid them. Communication within home networks can be generalized through mesh networking without going back to the access hub again and again. Consequently, network congestion occurring owed to backhaul access can be minimized. In this relevance, wireless mesh routers have no constraints on power consumptions and mobility. Accordingly, protocols projected for mobile ad hoc networks and wireless mesh networks are unmanageable to accomplish satisfactory performance in this application domain.

2. **Community and neighborhood networking**

   In a society, the generalized architecture for network access is based on cable or DSL connected to the Internet, and the last-hop is wireless by connecting a wireless router to a cable or DSL modem. This type of network access encounters several disadvantages, such as

   - Though the information exchange take place inside the society, all data passes from Internet. This considerably minimizes network resource consumption.
   - Large section of areas in between houses is not enclosed by wireless services.
   - A costly but high bandwidth gateway amongst several zones may not be shared and wireless services must be set up separately. As a consequence, network service prices are hiked.

- Only a single path may be accessible for one home to access the Internet or communicate with neighbors. WMNs tries to eliminate these drawbacks through flexible mesh connectivity's between homes.

3. **Enterprise networking**

   It is a network for small – scale network in a building, or a large scale network amid offices in multiple buildings. In the past, standard IEEE 802.11 wireless networks are extensively used in almost all offices. Nevertheless, these wireless networks are still secluded islands. Relations amongst them is achieved through wired Ethernet connections addition of backhaul access modems enhances capacity locally, but is unable to improve robustness to link failures, network congestion etc. An alternate to ethernet wires is replacing of access points by mesh routers. Various backhaul access modems is jointly shared among nodes in the entire network, and therefore, robustness and resource utilization of enterprise networks is enhanced. WMNs can be scaled up as the size of enterprise expands. It is typical to deploy WMNs for enterprise networking because of the dynamic topologies being involved. This model can be adopted for public and commercial service networking scenarios such as airports, hotels, shopping malls, convention centers, sport centers, etc.

4. **Metropolitan area network (MAN)**

   WMN have various advantages in MAN. The physical- layer transmission rate of a node in WMNs is much higher compared to other networks. As an instance, an IEEE 802.11g node can send data at a rate of 54 mbps. Additionally communication among the nodes in WMNs does not solely depend upon wired backbone being use as alike wired networks, e.g., cable or optical networks, wireless mesh MAN is an in cost alternative to broadband networking, especially in developing regions. Wireless mesh MAN enterprise covers larger area as compared to enterprise WMNs

5. **Transportation system**

   As an alternative for restricting IEEE 802.11 or 802.16 accesses to stations and stops, mesh networking technology can spread access into vehicles. Consequently, nearby passenger information services, real time monitoring of vehicles, and communications amid driver can be maintained. To enable such mesh networking for a transportation system, two crucial techniques are needed: the high-speed mobile backhaul between a vehicle (car, bus, or train) to the Internet and mobile mesh networks inside the vehicle.

6. **Building automation**

   Inside a building, a mixture of electrical devices including power, light, elevator, air conditioner, etc., need to be controlled and monitored. At present this task is taken care by wired networks, which is very costly due to the difficulty involved in positioning and maintenance of a wired network. Lately, different types of networks are being adopted to minimize the cost involved in such kind of networks. Nonetheless, this effort lacked in satisfactory performance yet is costly. If building automation and control networks access points are switched by mesh routers, the installation cost will be reduce radically.

7. **Medical and health**

   In a hospital or any emergency unit, patient's data need to be transmitted from one room to another for different purposes. Information exchange is typically broadband, as we know high resolution images and different periodical monitoring information creates large amount of redundant data. Conventional wired networks provides limited coverage. Wi-Fi based networks are dependent Ethernet connections, which have more system cost and high complexity but lacking the abilities to eradicate dead spots. Conversely, such issues doesn't exist in WMN.

8. **Security surveillance system**

   Security is one of the most important issue to be considered in WMN. Security surveillance systems turn out to be an inevitable for enterprise buildings, shopping malls, grocery stores, etc. as compared to other security networks deployment of WMNs is more viable solution at such locations for connecting various systems.

2.4 WMNs with respect to security

The major problem which arises in respect to securing the WMN is the lack of centralized trusted authority for distribution of keys because of the distributive nature of WMN and as a result of it huge amount of work is done to present an effective key management scheme which seeks an encryption key assignment such that the induced network is connected and well protected against potential attacks. [12] Kandah et al. in [13] proposed a key management scheme for heterogeneous sensor networks. Each high-end sensor is preloaded with M keys, and each low-end sensor is preloaded with L keys ($M \gg L$) in a pre-distribution phase, where the keys are randomly picked from a pool of keys P without replacement. Followed by the discovery phase, which is used to check if neighboring sensors have a shared key, and the key setup phase, which is used to find a shared key between any two neighboring sensors when the discovery phase returns that there is no common key between them. But the scheme used in this paper use the available number of keys (K) to be assigned among all the nodes, without generating too many unnecessary keys, and keeping the network as secure as possible.

In this paper all MRs use the same fixed transmission power ($R \geq 0$). They have used a undirected bi-connected graph G(V ;E) to model the wireless mesh network where V is the set ofn nodes and E is the set of m links in the network. For each pair of nodes (u; v), there exist anundirected edge e ϵ E if and only if

$d(u; v) < Ru$, where d(u; v) is the Euclidean distance between u and v, and Ru is the transmission range of node u.

The threat model described in this paper helps us in understanding that if a node is captured by some attacker then he can very easily perform eavesdropping on its neighbor nodes which have the same encryption key for transmitting the data, since in this model the keys are distributed randomly, therefore this drawback of passive eavesdropping is minimized in this paper.

The motivation for this paper was that in the earlier scheme nodes within a 2-hops neighboring range of any node were not considered, but in this paper the key assignment is done in such a way so that the probability of getting the same encryption key between any two neighboring nodes is minimized. Four factors on which the efficiency of this paper has been concluded;

1. (Shared encryption key (Sku,v)): Given any two neighboring nodes u, v ϵ G, if there is an encryption key k ϵ keys(u)$\cap$ keys(v), then we can say that there exists a shared encryption key Sku,v between node u and node v, where keys(u) and keys(v) are the sets of keys which are preloaded to node u and v respectively.

2. (2-hop compromised nodes (2CNu)): Given nodes u, v, w ϵ G, where v is a 1-hop neighbor of u, and w is a 2-hop neighbor of u via v. If node u has been compromised,the 2-hop compromised nodes of node u (2CNu) is defined as the set of nodes (w), for which node v sends messages encrypted by any key k ϵ Sku,v $\cap$ Skv,w.

3. (Node compromise ability (NCA(u))): Given a network G, we define the node compromise ability (NCA) for a compromised node u ϵ G, as the number of nodes in the set 2CNu. NCA(u) = —2CNu—.

4. (Malicious eavesdropping ability (MEA)): Given a network G with n nodes, where each node has been preloaded with a set of encryption keys. The

malicious eavesdropping ability in the network is defined as the maximum NCA among all nodes in G. MEA = maxNCA(n)—n ϵ G.

The aim of this paper is to reduce the MEA.

Algorithm 1 Secure Key Management Scheme (G, K)

```
for each node u $\epsilon$ G do
    keys(u) = $\varnothing$;
end for
for all nodes in G do
    for each node u $\epsilon$ G do
        Find NIR(u);
        Calculate —NIR(u)—;
    end for
    Choose node u $\epsilon$ G with the highest —NIR(u)—;
    for each node v $\epsilon$ NIR(u) do
        //Assign keys between node u and node v $\epsilon$ NIR(u) based on the following rules:
        if keys(u) = $\varnothing$ and keys(v) = $\varnothing$ then
            Choose k as the least used key from K;
            Add k to keys(u) and keys(v);
        else if keys(u) = $\varnothing$ and keys(v) = $\varnothing$then
            Choose k as the least used key from K not in keys(w), where w is a neighbor of u, if applicable, else choose k as the least used key from K;
            Add k to keys(u) and keys(v);
        else if keys(u) = $\varnothing$ and keys(v) = $\varnothing$ then
            Choose k as the least used key from K not on w where w $\epsilon$ NIR(u) $\cup$ NIR(v), if applicable, else choose the least used key from K;
            Add k to keys(u) and keys(v);
        end if
    end for
end for
```

Drawbacks of this paper:

1. This paper tries to minimize only one type of attack that is passive eavesdropping.

2. Static topology is being considered instead of dynamic.

2.5 WMN MAC-Layer Security

A secure MAC layer is responsible for ensuring that a mesh network carries traffic only for authorized stations.

2.5.1 Availability

802.11 don't report availability concerns. Instead, the self-healing property in 802.11s WMNs — a property shared with MANETs — allows the WMN to route traffic around congested areas automatically.

2.5.2 Fairness

802.11s partly solves the fairness problem by involving the standard contention based enhanced distributed channel access (EDCA).

2.5.3 Authentication

In conventional 802.11 networks, the difficult problem of authentication and key distribution is clearly outside the specification's scope. 802.11s handles it through the use of 802.11 PSK mode and implements a novel mechanism known as MKD-PSK. This needs a distinctive 256-bit PSK for separate station, which is collectively shared only with a trusted third party known as the mesh key distributor (MKD).

2.5.4 Authentication and Access-Control Protocols

802.11 uses the 802.1X port-based access-control mechanism to manage authentication exchange and initiate the four-way handshake used for key establishment.

802.1X is very effective in conventional infrastructure environments, but it has shortcomings when used for WMNs. The dual wireless authentication protocol (DWAP) protocol, is an efficient alternative that substantially reduces the overhead associated with 802.1X.

2.6 Hybrid Wireless Mesh Protocol

802.11s is unfamiliar in that the MAC layer is accountable for guaranteeing that a frame reaches its end point. In 802.11s, Hybrid Wireless Mesh Protocol (HWMP) accomplishes path selection at the MAC layer, and the protocol forwards frames at this layer.

2.6.1 Routing Attacks

To address these risks, researchers have proposed a number of secure routing protocols that use cryptography-based approaches to stop intruders.

2.6.2 Rushing attacks

Chang the route-discovery procedure to enhance the possibility that the intruder station is contained within in a given route. The purpose of this attack is to increase the probability that the adversary's station is contained within in a given route. The defense against this attack has two parts: a secure neighbour detection protocol and a alteration to the routing protocol's route-discovery reasoning.

2.6.3 Gray Holes and Black Holes

A black hole is a station that publicizes its inclination to take part in a route but forwards no data. A gray hole is a more challenging as it conditionally decides on which traffic it will transmitt. The wormhole attack creates a channel joining different parts of the network, thus tricking stations next to one end of the wormhole into trusting that they're neighbors with stations on other side. Zheng in [14] gave symmetric key management which is used for used for authentication in WMN it can also be used for safeguarding routing keys for on demand routing protocol. Here first a provisional route is set up between an IAP and wireless device, afterwards a secure routing key is transmitted from AP to wireless device via KDC. Therefore a secure routing operation can be started to launch secure routes among all Wireless devices which have gained the same secure routing key in the identical manner. Goal is to prevent a malicious user from trying to disturb data path routing functions or to cause genuine data packets to be wrongly routed.

There are two ways to secure data:

- Hop by hop
- End to end

On-demand routing protocols generate routes only when chosen by the source node. It initiates a fresh route discovery process inside the network. This procedure is accomplished once a route is set up or all possible route variations have been inspected. There are several ways in which an intruder can upset these normal on-demand routing procedures. Directing false route error messages in order to eradicate the working routes. Sending false route response messages in order to wage selective forwarding or sinkhole attack. Transforming the routing messages with inappropriate routing information. A security extension can be added to each routing message and recognition of the attack then can be attained.

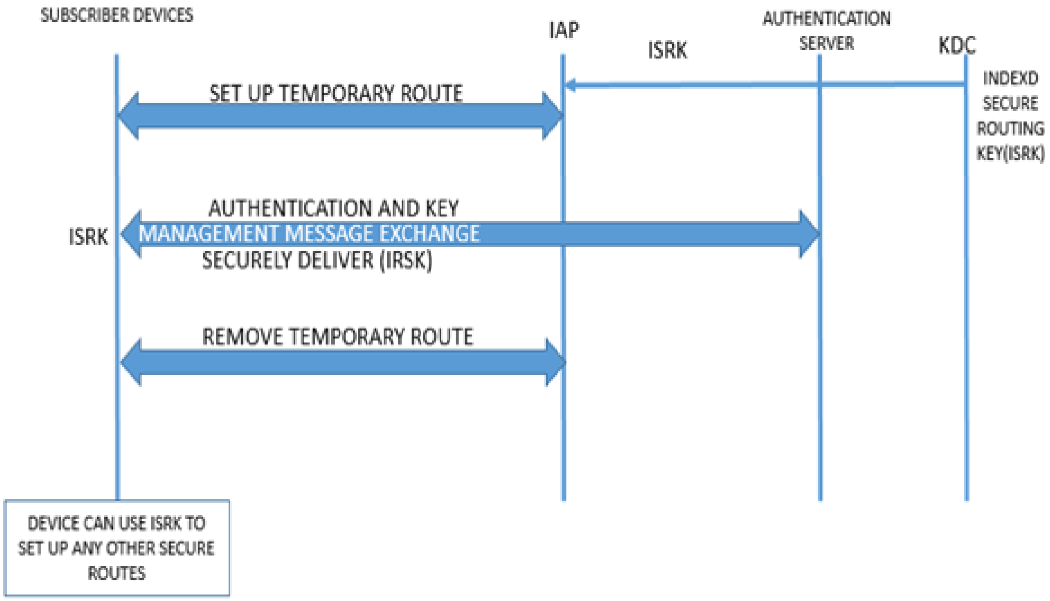


FIGURE 2.1: Message authentication in mobisec architecture (adapted from 14.)

Matignon et. al in [15] proposed MobiSEC, a comprehensive security architecture that delivers both access control for mesh users and routers as well as security and data confidentiality of all communications that take place in the WMN.

MobiSEC covers the IEEE 802.11i standard using the routing capabilities of mesh routers; after joining to the access network as common wireless clients, new mesh routers validate to a central server and obtains a temporary key that is used together to prove their identifications to neighbour nodes and to encrypt all the data transmitted on the wireless backbone links.

In this paper two key delivering protocol are used, named

1. Client driven protocol

In the client driven protocol the MRs obtain from the server a seed and a hash function type to produce the keys.

Assumptions: All nodes approved to join the wireless backbone have two licenses that demonstrate their identity: first is used through the certification phase that

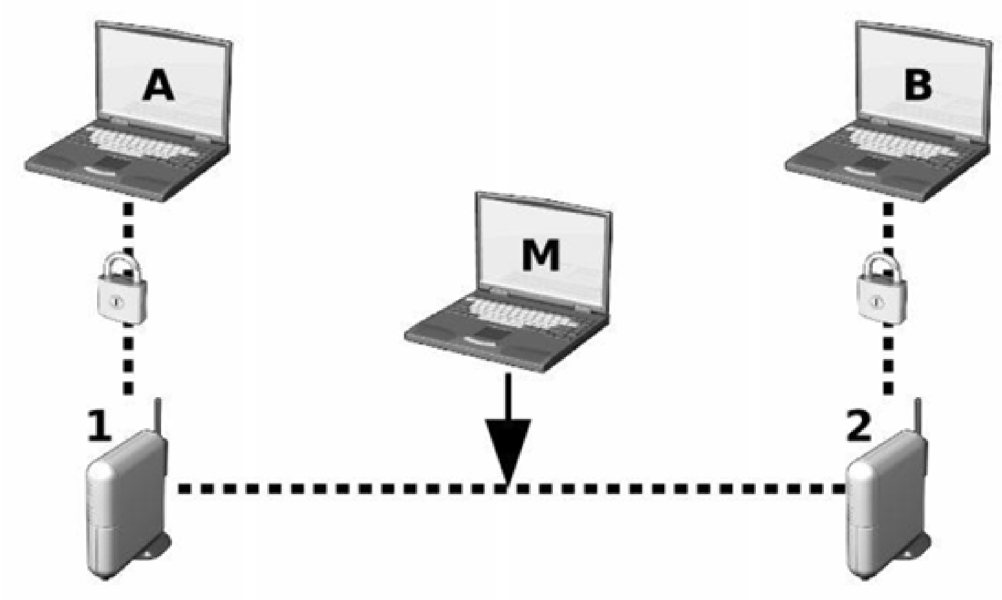


Figure 2.2: Client security (adapted from [15])

happens when a new node joins the network (we use EAP-TLS [4] for the 802.1X authentication, whereas the second credential is used for the mutual verification with the Key Server.

2. Server driven protocol: This protocol delivers a reactive method to distribute the keys used by all MRs. A common mesh router, after a positive mutual authentication with a central server, sends its first application to gain the key list used in the current session by the other mesh routers that form the wireless backbone and the time when it was produced, Key List Timestamp (TSKL).

Session: maximum validity time of the key list presently used by every node. The node, created on the instant in which it joins the backbone (tnow), can discover the key, amongst those in the list, currently used by its peers and its validity time (keyidx and T1) through to the following expression:

$$key_{idx} = \lfloor \frac{t_{now} - TS_{kl}}{timeout} \rfloor + 1 \tag{2.1}$$

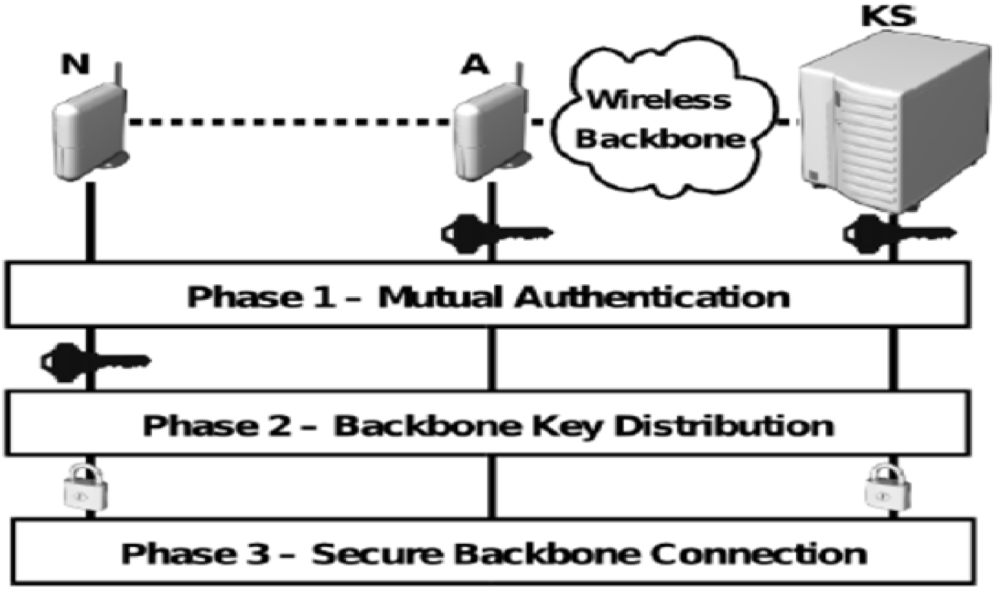

N
A
KS
Wireless Backbone
Phase 1 – Mutual Authentication
Phase 2 – Backbone Key Distribution
Phase 3 – Secure Backbone Connection

FIGURE 2.3: Backbone security adapted from [15]

$$T_1 = key_{idx}.timeout - (t_{now} - TS_{kl}) \tag{2.2}$$

The key index value that activates the proactive request to the server can be set equal to the difference between .the key list cardinality and a correction factor.

$$C = \lceil \frac{t_{last} - timeout}{timeout} \rceil, if t_{last} \geq timeout \tag{2.3}$$

$$C = 0, if t_{last} < timeout \tag{2.4}$$

$$t_{last} = t_r - t_s \tag{2.5}$$

Advantages

1. Architecture of MobiSEC is its independence from the basic wireless technology used by system nodes to form the backbone.
2. MobiSEC allows continuous movement to MCs and MRs.

Researches are being carried so as to reciprocate potential attacks by introducing secure routing technology [16], [17], intrusion detection technique [18], [19] and key management techniques [20], [21]. Sahbi Sassi, Mohamed Kassab, Abdel fettah Belghith & Jean Marie Bonnin [22], [23] proposed a technique in which they overcome the disadvantage of [24] i.e. Client mobility. The author proposed two authentication schemes one is proactive key distribution and other is PKD with IAPP caching. With this arrangement they were trying to fasten the secure the authentication procedure between mesh network and station.

M Parthasarathy [25] elaborate a technique, which define how a client can securely access the network along with confidentiality. In this technique, they use PANA and PAA agent, which are used to authenticate the client and build a tunnel into the network which helps to achieve confidentiality, integrity and also secure the exchanged confidential information.

Mustafa and Zhu. [26] [27] [28], work on a technique named Light weight hop by hop access protocol. The idea behind this is to authenticate mesh client and prevent the network from the resource consumption attack. In this authentication concept, the user's data are authenticated at each intermediate node before forwarding. LHAP best suited to adhoc network and resides between the data link layer, network layer and offers high grade protection.

CHAPTER 3

KEY MANAGEMENT SERVICES

In this chapter basic services provided by key management services are being described.

3.1 Key Setup

In the key setup phase, we define the global parameters necessary for cryptographic operations. Parameters such as key length, registration of user, generation of various keys, generation of security parameters etc., needs to be setup. This is an important phase in key management as all communicating parties are made to agree on the common security parameters before they can take part in secure communication.

3.2 Key Exchange

The most important service of a key management system is considered as key exchange. In this phase, depending on the type of keys being used, for instance in case of symmetric key system similar information/data is being exchanged. In the case of asymmetric key systems, we only need to exchange the public keys.

Although public keys can be exchanged in an open system but still there is a need of secure channel for exchanging symmetric key because if an interceptor gets the symmetric key, it would enable him/her to decrypt the cipher text.

3.3 Key Refresh

When the keys are used for a longer duration of time, an intruder may gain knowledge of the keys. To avoid or make such a situation inflexible for the adversary, the key management system provides the facility of refreshing the keys, where all the existing keys of the users should be refreshed to a fresh and unrelated keys. Related to it, the key management service should also make effectual and secure mechanisms to support dynamicity in the networks, such as adding of new users or deleting existing users to and from the network.

3.4 Key Revocation

Another important aspect of key management system is key revocation as it allows exclusion of compromised nodes from the network. Sometimes it may not be possible to completely prevent keys being negotiated under those situations, the key management system should arrange for mechanisms by which compromised keys of recognized nodes could be revoked or made impractical in the system.

3.5 Challenges of Key Management in WMNs

Disparate to other existing wireless networks, WMNs possess different types of constraints, which make the deployment of key management exceptionally challenging. Among other challenges, key management in WMNs has the following specific challenges:

- **Lack of physical security:** An opposition can easily capture a node and excerpt useful data including security key stored in the node's memory such as in mesh routers.
- **Wireless communication:** Broadcast nature of wireless communication makes it tougher to avoid unauthorized reception of the message.
- **Scalability:** WMNs can easily become congested. With the enlargement of network size, the complication of handling and supporting various protocols and keys in the network also rises.
- Scalability: The topology of the WMNs can changes vigorously, thus, centralized control is hard to attain. The key management protocol in WMNs has to reflect the information and become accustomed with the dynamic change of topology.
- Scalability: Limitations on resources such as memory, power, and computation in client nodes put supplementary challenges on the key management protocol in WMNs. Hence, resource aware key management techniques become a compulsion in WMNs.

3.6 Symmetric Key Management in WMNs

Symmetric key based schemes are most prevalent among researchers in WMNs, essentially due to their cheap computation times and less storage requirements. Consequently, many researchers have focused on providing possible solutions to key management problem in WMNs based on symmetric key based schemes [29] [30] [31]. Key managing schemes in wireless mesh network can be categorized as follows:(i) Single shared key schemes [29], (ii) Pair-wise key pre-distribution schemes [30], (iii) Trusted third-party based schemes [31].

3.6.1 Single Shared Key Schemes

Lai et al. [29] suggested an easy and effective key management way out for WMNs. In their pattern, a master key is pre distributed and kept inside each node in the system. A pairwise key can be set up by using this master key and a random number exchanged between each nodes. This scheme is immensely scalable and very attractive since it only requires one key to be stored in each node. Also new node addition is quite simple. However, the shortcoming of it is understandable. When the master key of a node is compromised it would negotiate all the pairwise keys of the network, and as a result the whole network would be conceded.Therefore, this scheme is resilient against node capturing. Besides, it does not offer any authentication as all nodes in the network uses the identical master key.

3.6.2 Pair-wise Key Pre distribution Schemes

Pairwise key pre distribution schemes use separate secret keys for each connection with different kind of nodes. Put in other words, if there are N nodes in the network, this scheme requires each node to store (N-1) discrete keys. Chen and Perrig [30] proposed a system in which a distinct pairwise key between each pair of sensors is pre-distributed and straight away stored in each node before deployment. Although this solution provides the most resilience against node capture, it is inefficient to deliver scalability. This means that when the network size becomes outsized, this scheme becomes infeasible for memory constrained nodes. Also it is not easy to add new nodes because every node has to store new key when any new node joins the network.

3.6.3 Trusted Third-party Based Schemes

In this scheme, a moderator node acts as a reliable node for any two nodes willing to communicate. Chan and Perrig [31] propose peer intermediaries for key establishment in sensor network called ”PIKE”, where the key establishment between two nodes is based on the mutual trust of a third node. For any two nodes of A and B, there is a node C that share a key with nodes A and B. The main drawback of this scheme is that sometimes it may be difficult to find such moderator node in the wireless network.

3.7 Asymmetric Key Management in WMNs

Many researchers expect that asymmetric key based schemes are computationally costly for WMNs because of their constraints. However, driven by current progress and optimization of cryptographic algorithms, numerous research groups have revealed striking outcomes which indicate asymmetric key scheme can also be used in wireless mesh networks.

3.7.1 RSA-based Key Management for WMNs

A remarkable RSA-based public key scheme has been proposed by Watro et al. [32] called TinyPK. It sanctions authentication and key agreement between resource constrained nodes. This scheme is using basic RSA to generate private and public key pair for each node in the network. It is being assumed that there is a certification authority (CA) offered before the beginning of the protocol and any party that wishes to communicate with the nodes also requires its own public/private key pair and must have its public key signed by the CA’s private key, thus establishing its individuality. To perform authentication, the exterior party submits its signed public key and some text signed with its private key. The protocol operation starts when the third party provides a challenge to the network. This challenge involves two parts: the first part involves the public key of the node, signed by the CA's private key; the second is a complex entity consisting of a nonce (a time-stamp) and a message checksum, signed with the third party's own private key. This information is directed as clear text and the nonce serves to detect any replay attacks, wherein a intruding party archives previous effective messages and re-broadcasts the message in order to provide false documentation or otherwise attack a system. The checksum is computed to certify integrity of message.

After reception of the message by some another node, it uses the preloaded CA public key to authenticate the first part of the task and extract the third party's public key. This public key is later usedvalidatethe second part of the message and extract the nonce and checksum. The nonce and checksumare authorized. If they pass validation, the third party has been effectively authenticated to thewireless network and is well-thought-of an approvedunit for wireless data. Then, the node uses this key to encrypt the session key plus the received nonce using the third party's public key. Next this, the message is directed back to the third party, which decrypts it using its private key, verifies that the nonce is the same as the one it sent, and if so, can record the session key for upcoming session.

3.7.2 ID-based Key Management in WSNs

The impulse of identity-based encryption is to make the certificate-based public key encryption system simpler. In the certificate-based public key encryption system, calculation increases when a user has to certify another user's certificate before using his/her public key. As a result, each user wants a huge storage and computing time to store and validate each other's public keys and the equivalent certificate. The rudimentarynotion of the identity-based encryption scheme is that arandomly chosen string is considered as a public key. As a consequence, a user can use any ID, such as email, to calculate a public key, rather than mining from the certificate distributed by a certificate authority. Shamir first familiarized identity based cryptography to shorten the management of public keys in a public key based cryptosystem. Though his idea was very attractive, for a lengthy time it was an open research problem to obtain an efficient and secure IBE scheme. Recently Boneh and Franklin [33] in the same,were proficient to come up with hopeful results to use the IBE scheme in different cryptographic applications. The building blocks of IBE is based on the concept of bilinear pairing — or pairing for short. The followings are necessary facts about the pairing

- G1, G2 and GT are multiplicative groups of prime order p.
- g1 is a generator of G1and g2 is a generator of G2.
- Z is an isomorphism from G2 to G1 with Z (g2) = g1. The map e must have the following properties:
- Bilinear : $\forall$ u ϵ G1, $\forall$ v ϵ G2 and $\forall$ a, b ϵ Z we have e(ua, vb) = e (u, v)ab
- Non-degenerate e: (g1, g2) $\neq$ 1.
- Computable: there is an efficient algorithm to compute e (u, v) for all u ϵ G1 and v ϵ G2.
- A map always exists, but the matter here is whether or not it can be proficiently computed within an acceptable time limit. For the sake of simplicity and without loss of generality we could write g1 = g2 i.e., G1 = G2 = G. Using the IBE, it is promising to project a non-interactive secure key distribution scheme for WMNs, where each node is given a exclusive ID and a exclusive secret, not made public with any other object in the network.

3.8 General discussion

Although symmetric key schemes are light-weight and widely used in WMNs, there are some distinguishedshortcomings. Initially, managing the keys and approving on a shared key requires additional overhead. Secondly, the key pre-distribution methodology usually cannot assure complete connectivity of the network even with high deployment density. Finally, symmetric key cryptosystems sometimes becomes unsuccessful to provide authentication for the cooperating parties. In contrast, in asymmetric key schemes, communicating parties only have one pair of keys namely, the private and public key. This scheme is scalable and provides authentication service effortlessly. This convenience however comes at a price: a technique for authenticating the public key must be provided. This is conventionally been done by introducing a trusted CA and authenticating digitally signed certificate by the CA, which is a computationally costly operation [33]. However, using an ID-based scheme, known facts that exclusively recognizes the user can be used to derive its public key. As a result, keys are self-authenticated here, the only constraint is that the ID of the user has to be unique and only a reliable authority should be able to generate the ID.

In this thesis, we propose a hybrid solution to the key management problem in WMNs where we combine the symmetric key-distribution scheme with pairing-based scheme to provide efficient and scalable key management protocol. Although we have combined pairing-based technique in the proposed scheme, it is used rarely, so that the overall computational overhead of pairing-based calculations are minimized. The proposed key management protocol supports multiple types of networks and provide scalability without increasing memory overhead.

CHAPTER 4

BACKGROUND KNOWLEDGE

In this chapter, we intricate the background techniques used in the proposed key management protocol. First we elaborate the identity-based encryption schemes [34] and provide their security analysis. Following this we elaborate symmetric key distribution technique and discuss its strong point.

4.1 Identity-based Encryption

General Overview of IBE

IBE is a new form of public-key encryption technology that permits a user to compute a public key from a random string. One can alter the arbitrary string to avoid a user having the same IBE key endlessly. Typically, it is beneficial to include some information about the user's identity or validity period of the key in the string. The facility to calculate keys as needed gives IBE systems different properties than those of conventional public-key systems, and these properties offer substantial practical benefits in some situations. Even though there are undoubtedly few situations in which it is unmanageable to solve any problem with traditional public-key technologies that can be solved with IBE, the solutions that use IBE may be much easier to implement and less costly.

In a regular public-key system, both the user and an agent working on behalf of user arbitrarily generates public-private key pair. After it is made, the public key, alongside with the user's identity need to be enumerated with a CA. The CA is answerable to approve the authenticity of the user's personal information before it can digitally sign the user's public key to generate a digital certificate. A duplicate copy of the digital certificate is then sent to the possessor of the private key and the same copy is kept in a public certificate repository that is available to others who might want to get a user's key. The confirmation of the user's identity is cautiously handled by the CA before a digital certificate is issued to the user, a process that is typically very costly. The procedure of generating public-private key pairs is also computationally expensive. Generating two 512-bit prime numbers that are suitable for use in creating a 1, 024-bit RSA private key is certainly practicable, but generating larger primes gets gradually more expensive [34]. Creating two 7, 680-bit primes that are suitable for use in creating a 15, 360-bit RSA private key is not an operation that widely used computers can easily perform, yet such keys are needed to securely transport the 256-bit AES keys that are used in modern period [34]. Since generating keys and verifying user's identities can be costly calculation, digital certificates are generally issued with fairly long validity periods, over a period of one to three years. Due to the relatively long validity period of the public keys managed by digital certificates, it is often required to veriy the key in a certificate for validity before using it. To use the public key that is signed by a CA, a user must verify that the certificate is not terminated or withdrawn. This can be achieved either by sending queries to the public repository for new certificate or by inspecting the list of discarded certificates or by querying an online service that returns validity status of the certificate. After any essential validity inspection is done, the user can use the public key to encrypt information and transmit it to the owner of the pubic key. Since only the beneficiary has the private key corresponding to the public key, he can decrypt and get the information [34].

An IBE system has resemblances with customary public-key systems. However,

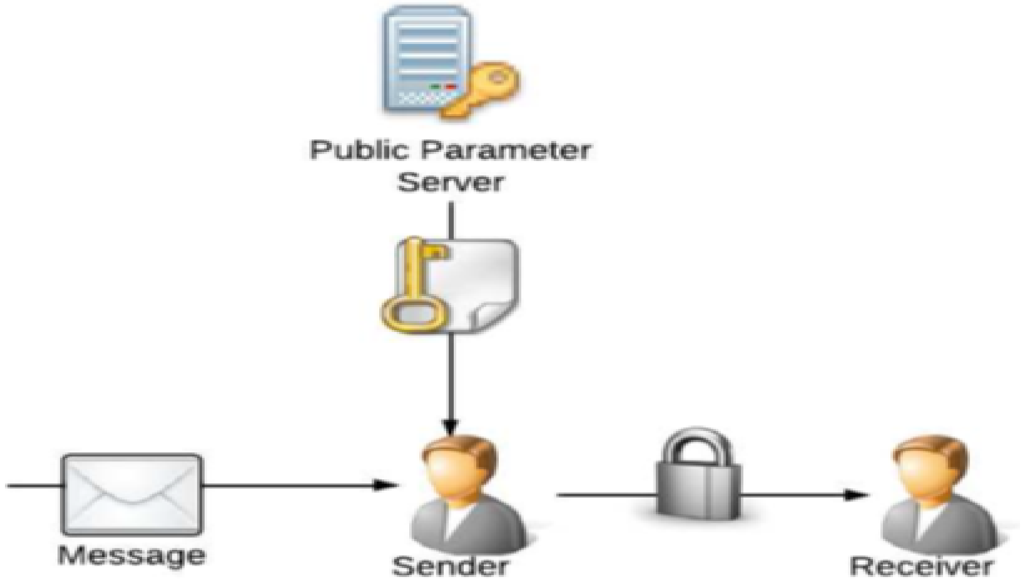


Figure 4.1: Generation of keys in an IBE system. (Adapted from [34].)

it can be different in other ways. While in conevntional public-key system, the certificate comprises all the necessary constraints to use the key, to use an IBE system, typically a user needs to communicate a trusted third party and get all the compulsory factors to generate the key after receiving the necessary parameters, after acquiring the essential parameter the public key it can generate public key of any user and can use it to encrypt the data.

After receiving an IBE encrypted message, the receiving party contacts PKG and verifies himself in a particular way. The PKG is a trusted component accountable for generation of IBE private key that matches to the IBE public key used to generate the encrypted message. The PKG typically uses some secret information called master key and user's information to generate the IBE private key. After the private key is generated, it is securely distributed to the authenticated user. The authenticated user then uses the IBE private key to decrypt the information. This is shown in Figure.

The building blocks of IBE is based on the concept of bilinear pairing — or pairing for short.

4.1.1 Boneh-Franklin IBE Scheme:

So, after calculating the shared secret $e(P, P)^{rst}$ Alice hashes the shared secret into a format compatible with the plain text. The value of $e(P, P)^{rst}t$ is an element of some Fq, for example, while a typical message is an element of $(0, 1)^*$, so that $e(P, P)^{rst}$ needs to be mapped into $(0, 1)^*$ so that it can be combined with the plain text to produce the cipher text. So, Alice hashes the shared secret $e(P, P)^{rst}$ to the message space and combines the resulting hash with the plain text M to get the cipher text $C = M \bigoplus Hash(e(P, P)^{rst})$. Bob then calculates the shared secret $e(P, P)^{rst}$ hashes it to the message space, and recovers $M = C \bigoplus Hash(e(P, P)^{rst})$. In Algorithms 2, 3, 4, 5, we provide the summary of the steps in Boneh Franklin IBE scheme.

Algorithm 2 Boneh-Franklin IBE Setup adapted from [34]

```
Require: A security parameter k, an elliptic curve E, a plaintext bit length n.
Ensure: BFParams = (G1,GT , e , n, P, sP,H1,H2,H3,H4) and master secret s.
Select a prime p and prime power q with $p|\#E(Fq)$ and $p2|\#E(Fq)$ and such that the bit security level provided by p and q meets the required security parameter k. For best performance, p should be a Solinas prime.
Select a random $P \epsilon E(Fq)[p]$ and let $G1 =< P >$.
Let k be the embedding degree of $E/Fq$; select a pairing e : $G1 \times G1 \to F^*_{qk}$
Let $GT =< e < P, P >>$.
Select a random $s \epsilon Z^*$ and calculate sP.
Select appropriate cryptographic hash functions H1 : $0, 1^* \to G1$ , H2 :$GT \to 0, 1^n$ , H3 : $0, 1^n 0, 1^n \to Z^*p$ and H4 : $0, 1^n \times 0, 1^n \to Z^*p$.
The master secret is the value s.
The public parameters are BFParams = (G1,GT , e, n, P, sP,H1,H2,H3,H4).
```

Algorithm 3 Boneh-Franklin Key Extraction adapted from [34]

```
Require: A string ID representing an identity and a set of public parameters
    BFParams = (G1,GT , e, n, P, sP,H1,H2,H3,H4).
Ensure: The private key sQID.
Calculate sQID = sH1(ID).
```

4.2 Security of IBE

Note that we can write QID = tP for some (unknown) t, so we have $e(rQID, sP) = e(rtP, sP) = e(P, P)e^{rst}$ So, we can also think of the ciphertext as being C = $(rP, M \oplus H2(e(P, P)^{rst}))$. An adversary can obtain P and sP from the public parameters, can calculate QID = tP from the recipients identity, and observes rP in the ciphertext. If he can calculate $e(P, P)^{rst}$ from P, rP, sP, and tP then he can recover the plaintext message M by calculating $(M \oplus H2((e(P, P)^{rst})) \oplus H2(e(P, P)^{rst} = M$, but calculating $e(P, P)^{rst}$ in this way is exactly the BDHP.

Algorithm 4 Boneh-Franklin Encryption adapted from [34]

```
Require: A plaintext message M of length n bits, a string ID representing the
    identity of the recipient of the ciphertext, a set of public parameters BFParams
    = (G1,GT , e, n, P, sP,H1,H2,H3,H4).
Ensure: A ciphertext C = (C1,C2,C3).
Calculate QID = H1(ID).
Select a random $\sigma\epsilon 0, 1n$.
Calculate $r = H3(\sigma, M)$.
Calculate C1 = rP.
Calculate $C2 = \sigma \oplus H2(e(rQID, sP))$.
Calculate $C3 = M \oplus H4(\sigma)$.
```

Algorithm 5 Boneh-Franklin Decryption adapted from [34]

```
Require: A ciphertext C = (C1,C2,C3), a set of public parameters BFParams =
    (G1,GT, e, n, P, sP,H1,H2,H3,H4), a private key sQID.
Ensure: A plaintext message M or an error condition.
Calculate $C2 \oplus H2(e(sQID, C1))$.
Calculate $M = C3 \oplus H4(\sigma)$.
Calculate $r = H3(\sigma, M)$ and then calculate rP. If $C1 \neq rP$ then raise an error
    condition that indicates an invalid ciphertext. Otherwise, return the plaintext
    M.
```

So, if the BDHP is sufficiently difficult, then it will be difficult for an adversary to recover a plaintext message from a corresponding ciphertext.

Although IBE is a very interesting technique, it has some shortcomings. IBE requires incessant availability of the PKG and PKG needed to be trusted by all the users. It also requires some sort of secure and authenticated channel between PKG and a user to send the IBE private key. In the context of the Internet these requirements are difficult to implement and therefore IBE has not been very attractive solutions in Internet. However, this is not a problem in WMNs. Usually, WMNs are deployed and managed by a single authority and a centralized control is assumed through the base station node.

4.3 Key distribution scheme

In this scheme [35] we are assuming that each user is sharing a unique master key with trusted third party. Hence to obtain a session key following steps would be executed:

1. A node issues a request to TTP/MRs which includes the identity of both the nodes and a nonce (random value to secure the network).
2. TTP/MRs on receiving the request sends the secret key encrypted with node1 master key and some additional information intended for node2, while the information intended for node2 is encrypted using master key of node2.
3. Node1 keeps the session key with itself forwarding the information for node2.
4. On receiving the information from node1, node2 verifies the information intended for it.
5. Now node2 knows the session key, knows other party is node1 and hence the communication among them begins.

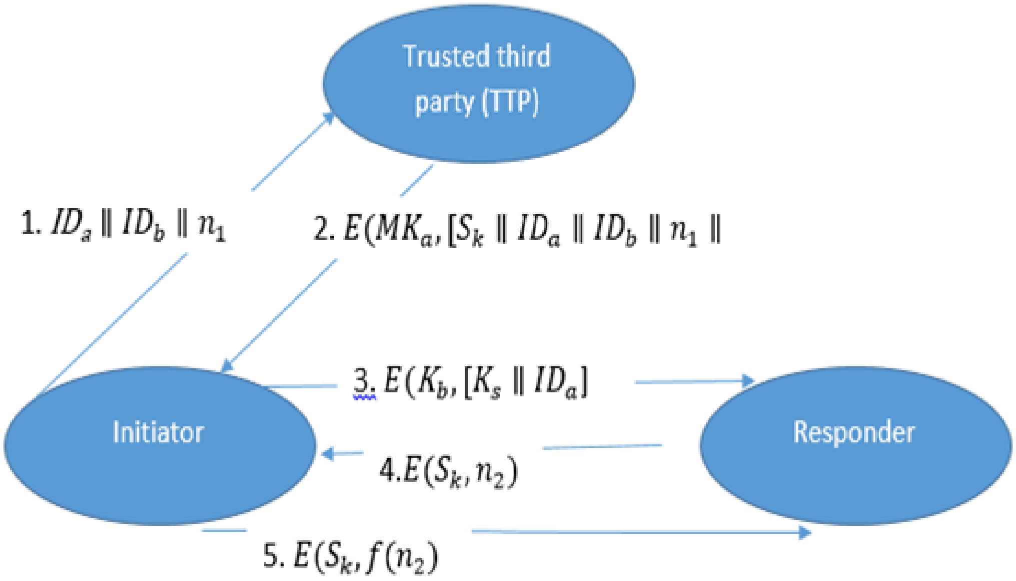

Trusted third party (TTP)
1. $ID_a \parallel ID_b \parallel n_1$
2. $E(MK_a, [S_k \parallel ID_a \parallel ID_b \parallel n_1 \parallel$
Initiator
3. $E(K_b, [K_s \parallel ID_a]$
Responder
4.$E(S_k, n_2)$
5. $E(S_k, f(n_2)$

Figure 4.2: Symmetric Key Exchange Method

6. For further security concerns node2 sends a nonce with their current session key to node1, upon receiving this nonce node1 alters this nonce by applying a random function and sends it back to node2 by encrypting it with its session key.

7. When the session is over keys are discarded.

Above scenario is depicted in the figure 4.2:

CHAPTER 5

PROPOSED KEY MANAGEMENT PROTOCOL

5.1 Optimized key management in Wireless mesh Networks

Above mentioned literature survey discusses the various key management approaches for securing the WMNs. The two basic key management techniques are symmetric and asymmetric key management. Asymmetric key management are very secure though they suffers from high computation overhead and also require more storage space. Even though in symmetric key management techniques less computation is required it may require more storage, but if we consider the case of WMNs we require enhanced security at the cost of less computation because of the restriction on utilization of resources. Therefore, the use of any single key management techniques to secure WMNs is not a suitable approach for real time application. Therefor we are proposing a hybrid approach to secure the network. By using IBC for the initialization phase which is a slight variation of PKI significant difference can be realized. And then session keys among the users are generated for secure communication. The symmetric method for generating session keys for communication is more suitable in WMNs as it avoids the very basic

Table 5.1: Notations used

MC	Mesh Clients
MR	Mesh Routers
GW	Mesh Gateways
TA	Trusted Authority
MK	Secret Master Key
SK	Session Key
ID_x	ID of Node x
N	Nonce
$f(N)_n$	Function on nonce

attacks in the wireless networks. And the storage space is reduced as the keys are discarded once the session is over. All the notation which we have used in our approach are being described in table 5.1.

5.2 Overview and assumptions

In our proposed scheme, we assume that all clients' nodes are homogeneous in terms of computational capabilities and memory capacities. Although we assume a hierarchical deployment structure where a trusted third party will manage the routers and clients. Trusted third party is considered secured from adversaries.

5.3 Proposed architecture

We have considered a hierarchical architecture of wireless mesh networks as depicted in figure 1.1. Wireless mesh networks consists of mesh routers which forms the backbone for the networks and are stationary but not fully secured while the mesh clients are provided with mobility facility and have access the network through mesh routers. The mesh clients forms the lower layer of the hierarchical model and mesh routes makes the intermediate layer. On the top a trusted third

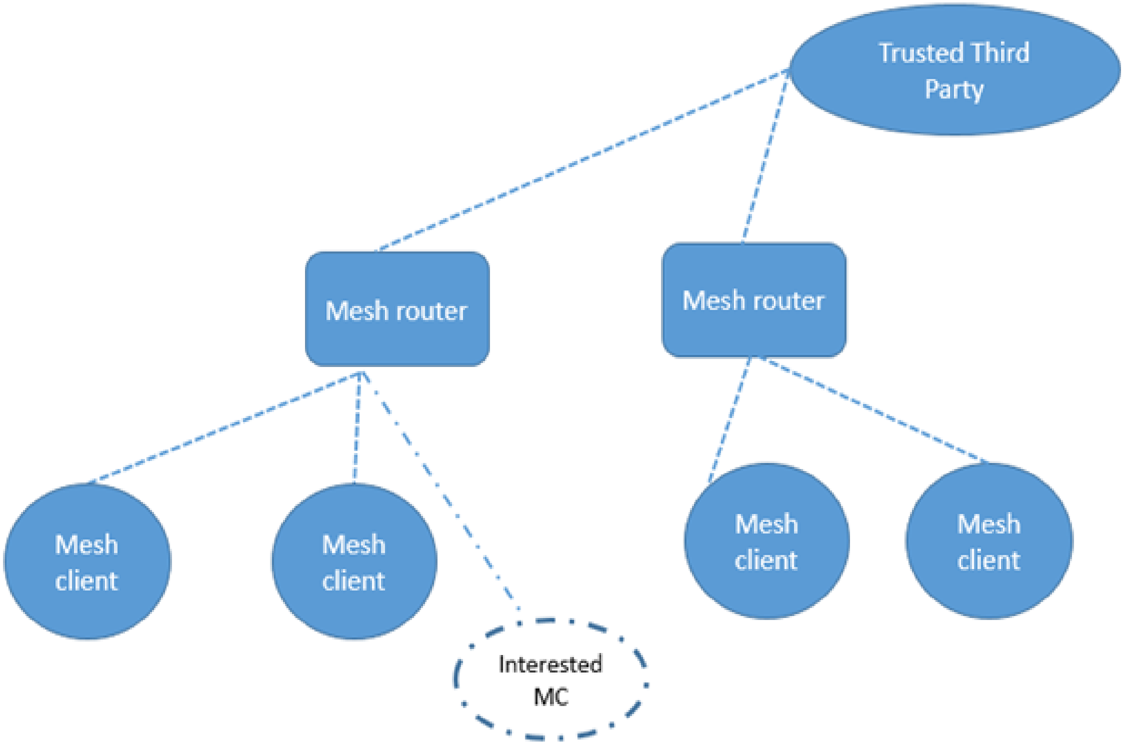


FIGURE 5.1: Proposed architecture

party exists whose function is to generate the keys and distribute it securely to the users. In order to enhance security the trusted third party is kept at a secure place hidden from clients. The considered architecture is shown in figure 5.1.

In our proposed approach, any client that wishes to be a part of a network, primarily have to contact with MRs. Equally, we are using an identity based encryption, in which each node has to place forth its own public key, i.e. Its own identity. The MCs use its own public key and the master public key obtained from MRs to generate the session key. Since most of the key management techniques consumes a lot of storage if we are storing pre deployment knowledge in nodes to generate the keys so in order to reduce the storage overhead we will compute the keys only at the time of requirement

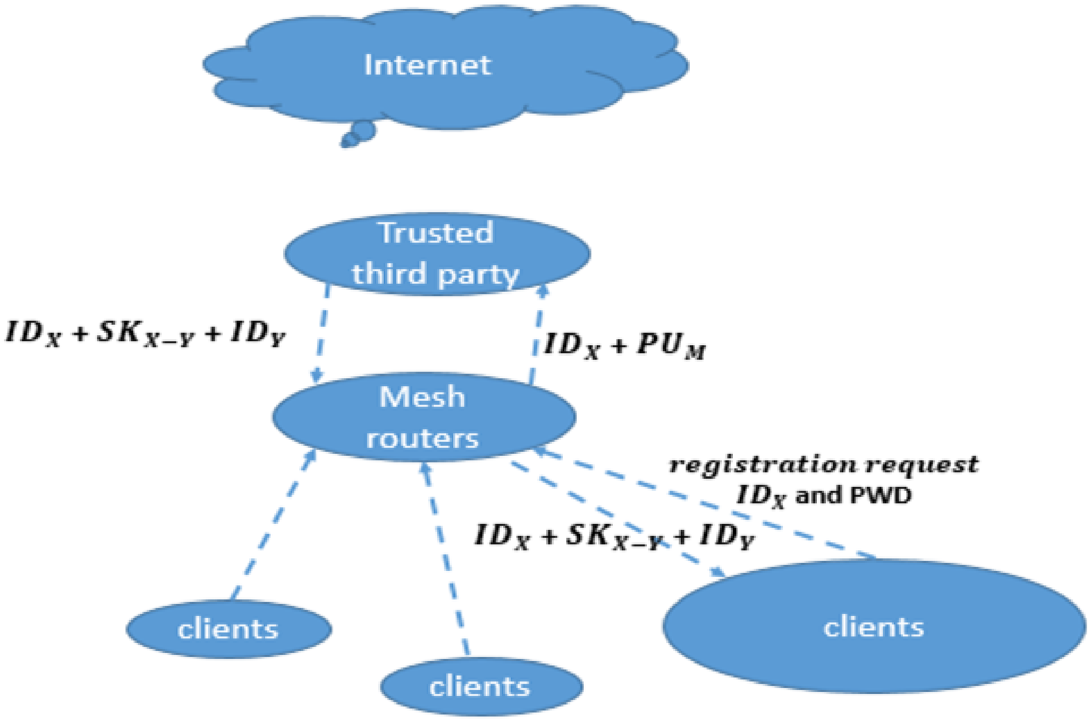


FIGURE 5.2: Key extraction for symmetric key exchange

5.4 Flow Diagram of Optimized key management in Wireless mesh Networks

In this section we will elaborate the proposed key management technique suitable for WMNs. Which incorporates the identity based encryption algorithm with symmetric key management technique and have further described the key management technique in sequential order.

Initially if a broker choose to join the network he will register itself to the mesh routers. The work trusted third party is to distribute a public master key to every client through mesh routers. Now if any user wishes to communicate to another user he will forward his identity along with the master public key and the identity of other user to the MR. This scenario is shown in figure 5.2.

After the extraction of key by a particular node the symmetric key exchange take place among the client nodes, we are using the IBE along with trusted third party only for initial key exchange and making the system more secure as TTP is not available to the public, therefore it is hard for an intruder to attack it .And the further key management and distribution is explained in next section.

5.5 Key Establishment and Distribution

1. Every node gains its unique secret master key for communicating with peer nodes through identity based cryptography explained in the above section.
2. After gaining the unique secret master key from trusted parties, a typical scenario for symmetric key establishment and distribution is being described here which would help in securing the wireless connection. Instead of distributing the available number of keys as in [10], we will secure the links by establishing the session keys for a session between any two peer nodes. The session keys can be established between any clients, between any two routers and between router and a client, in this manner entire network is being secured. Every node in this architecture shares a master key with the trusted parties.

Now if any client wants to establish a session for securely transmitting their data, they would communicate in the following order:

1. $ID_a \| ID_b \| n1$

   Node A in order to establish connection with nod B issues a request to trusted party. The request involves the identity of A and B along with a nonce (unique identifier) which is a random number and is different for every request.

2. $E(MK_a, [S_k \| ID_a \| ID_b \| n_1 \|] E(MK_b, [S_k ID_a])$

   The trusted party responds to node A by encrypting the message with his master key. This message is intended for both A and B.

A. As it is encrypted using master key of A, only node A can read it, and it the includes session key to be used for this session along with the original message, so as to enable A to match the this with original request.

B. For node B it contains a message encrypted with master key of B along with the session key and identity of A.

Node A store the session key and forwards the message intended for node B.

1. Now session key have been exchanged securely between both the parties and they exchange their confidential securely.
2. $E(S_k, n_2)$

   For keeping the session alive nod B will ping the node A with their current session key and with a different nonce n_2.
3. $E(S_k, f(n_2))$

   Node A responds to node B by altering the nonce $f(n_2)$ and then encrypting it with their session key which ensures B that previous message was not a replay message.

The last two messages are authentication messages while top three messages are key distribution messages. We have extended the above technique for establishing a secure channel between two nodes belonging to different domains.

1. $ID_a \| ID_b \| ID_{MR1} \| ID_{MR2} \| n_1 \| n'_1$

   Upon receiving the following message from node A, if trusted party does not have the associated identity of node B, it will broadcast the above message to nearby routers.

2. The router having the identity of B respond to its associated router and client. The client is addressed by trusted party as:

    - $E[Mk_b, (ID_{MR2} \| ID_b \| ID_a \| Sk_{r-c} \| n_1$

      The mesh router having the identity of node B, sends the message to node B by encrypting that message with master key of node B, so that only node B can access it. While the message includes the identity of node A, B and of the associated trusted party, along with the original nonce send by node A, and a share key which is to be utilized between MR2 and node B.

      At the same time MR2 sends a message to MR1 as:

    - $E[Mk_{MR}, (SK_{MR}(ID_a \| ID_b \| ID_{MR1} ID_{MR2} \| n'_1 n''_1$

      Trusted parties establish the session key among themselves by exchanging the session key created by accessed trusted party. The message include the identities of node A, B and the involved routers with a new nonce n'_1. A new nonce is being exchanged to show creation of new session.

3. Till now session key have been established between MR1 and MR2 and between MR2 and MC2. In order to establish the full secure connection MR1 and MC2 responds to MR2. Client node responds to trusted party as:

    - $E(SK_{R-c}, [ID_b \| ID_{MR2} \| n_1 \| f(n''_1)])$

      Client authenticate to router of receiving the share key by altering the nonce intended for their session and encrypting the message with their session key. MR1 respond to the MR2 as:

    - $E(SK_{MR}, [f(n'_1)])$

      Altering the nonce and forwarding it after encrypting by their session key, authenticate a session between the trusted parties through which node A and B can communicate securely.

4. MR2 sends a message to MR1 showing the willingness of node B to establish the connection with node A. The message also contains modified nonce intended only for node A, who wishes to establish the connection with node B.

   - $E(SK_{MR}, [ID_b \| ID_{MR2} \| ID_{MR1} ID_a \| f(n)_1])$

5. Upon receiving this message from MR2, MR1 forwards this request to MC1 as:

   - $E(MK_(a), [ID_{MR1} \| ID_{MR2} \| ID_a \| ID_b \| SK_{R-C} \| f(n)_1])$.

The message is encrypted using the master key of node A, so that only node A can read it, and it also contains the modified nonce so to avoid the replay attacks possible during this process.

After successfully exchange of these messages node A can communicate with node B and as soon as any of the node wishes to leave the session, whole of the session is being dissolved and the keys are discarded.

Since we are using symmetric key management techniques so in order to further enhance the security we are using the advance encryption standard (AES) technique to securely transmit the data between communicating parties.As in symmetric-key cryptography, the key is being shared among sender and the receiver. The sender applies the encryption function AES using the derived session keyto obtain the ciphertext produced from plaintext. The ciphertext is the transmitted to the receiver, who then applies the decryptionfunction using the same session key. Since the plaintext could not be obtained from the ciphertext without acquaintance of the key, the ciphertext is now ready to be sent public networks such as the Internet.

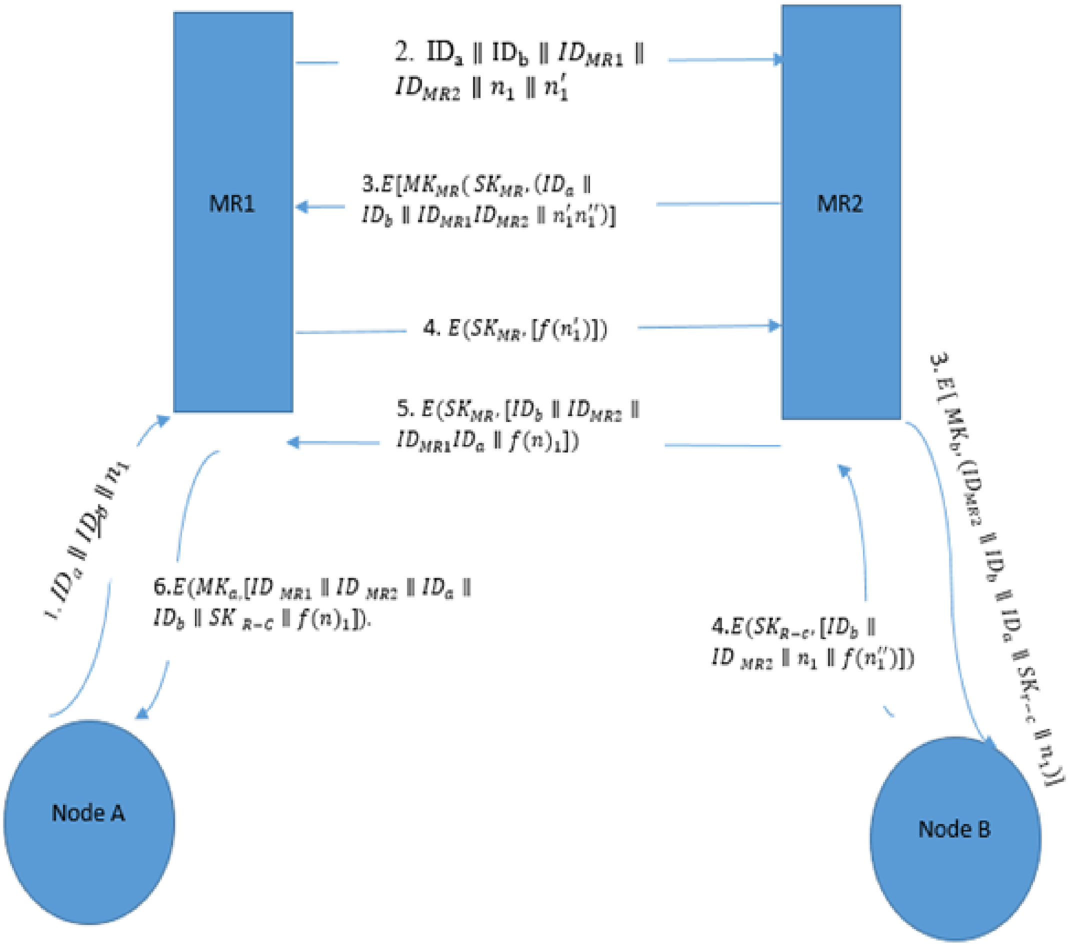

MR1
MR2
2. $ID_a \parallel ID_b \parallel ID_{MR1} \parallel ID_{MR2} \parallel n_1 \parallel n_1'$
3.$E[MK_{MR}(SK_{MR}, (ID_a \parallel ID_b \parallel ID_{MR1}ID_{MR2} \parallel n_1'n_1'')]$
4. $E(SK_{MR}, [f(n_1')])$
5. $E(SK_{MR}, [ID_b \parallel ID_{MR2} \parallel ID_{MR1}ID_a \parallel f(n)_1])$
1. $ID_a \parallel ID_b \parallel n_1$
6.$E(MK_a, [ID_{MR1} \parallel ID_{MR2} \parallel ID_a \parallel ID_b \parallel SK_{R-c} \parallel f(n)_1])$.
3.$E[MK_b, (ID_{MR2} \parallel ID_b \parallel ID_a \parallel SK_{r-c} \parallel n_1)]$
4.$E(SK_{R-c}, [ID_b \parallel ID_{MR2} \parallel n_1 \parallel f(n_1'')])$
Node A
Node B

Figure 5.3: Message exchange between two nodes belonging to different domains

CHAPTER 6

IMPLEMENTATION AND RESULTS

In this chapter we are describing about the methodologies being adopted in order to complete this research work and will compare this work to other existing approaches to measure the performance. We will also describe the various performance metrics which are considered to measure the network performance. The software used for this purpose is **NetBeans IDE 7.4** for front end and for back end we are using the **Mysql-connector-java-5.1.23-bin**. For the implementation we have considered the architecture consisting of a trusted third party, mesh router and mesh clients.

The MC in order to join the network communicates with the mesh router which authenticates the user using handshake process, if the authentication process is successful, the further request for key generation is sent to trusted third party. TTP then distributes the key to the communicating parties and establishes the session between interested parties. Addition to it we will be using AES to encrypt the data which needs to be exchanged in order to further enhance the security.

The parameters defined for measuring the performance of networks as are:

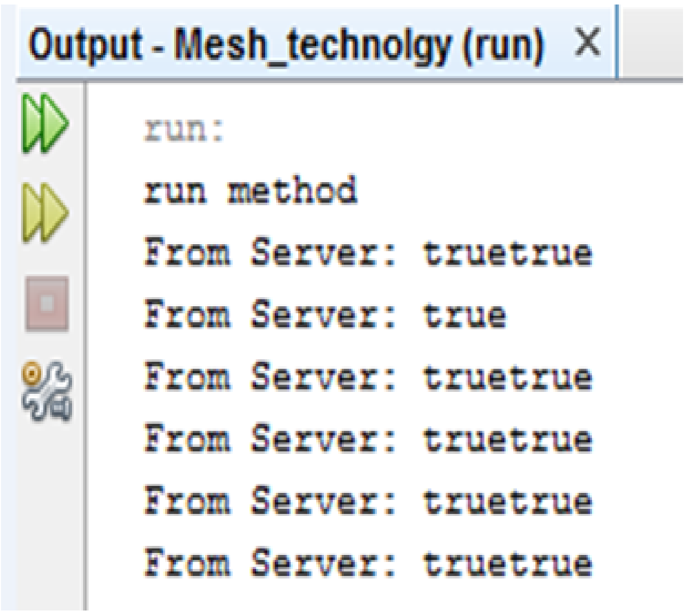
- **Throughput:** Throughput is used to measure the number of bits successfully delivered in per unit of time. It helps us in assessing the network in terms of its efficiency. Higher throughput signifies better network performance.

- **Key generation time:** It is the time elapsed after the successful user authentication and before the key is delivered to the mesh router. It should be minimum, as it is during this phase most the attacks are possible.
- **Encryption time:** It is the time required to convert the plaintext into ciphertext and put on the link. Higher encryption time enhances the probability of attacks on the network.
- **Delay time:** The time elapsed between the user request to join the network up to successful communication between the communicating parties. This time is fluctuating because of the involuntary actions carried out in the networks, such as signal loss, power down.

The research is carried out in three phase, in first phase the client sends request to mesh router in order to connect with the network. For performing this action client invokes the mesh router, on receiving the request router first registers itself or login if it is existing user. Router performs the authentication function on the mesh client by invoking the handshake process. With help of this procedure an intruder could be found out, since an intruder does not have the capability of performing hand shake process to the routers. In figure 6.1 Handshake process for an authenticated user have been shown.

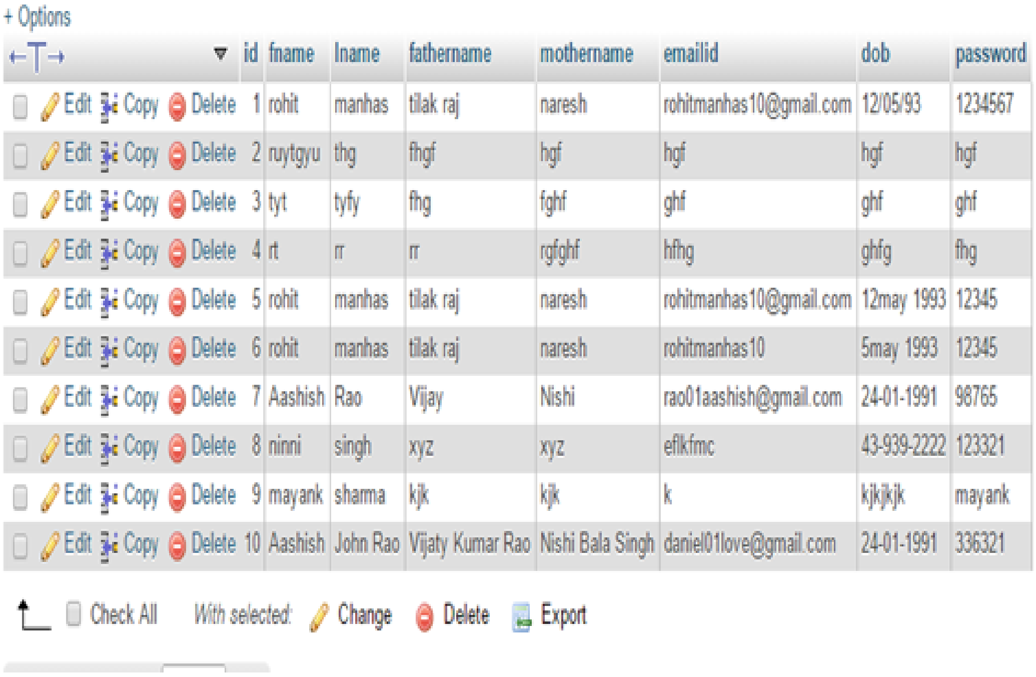
After the successful authentication process the client information is stored at the back hand at MySql server, as depicted in figure 6.2. The information is kept secured and is not exposed to any other user.

In the second phase, after the user is registered as an authenticated user and his credentials are maintained at the router, the router contacts to trusted third party to obtain the key, the TTP generates the session key to be used among the interested parties. After the client acquires a key he is able to participate in



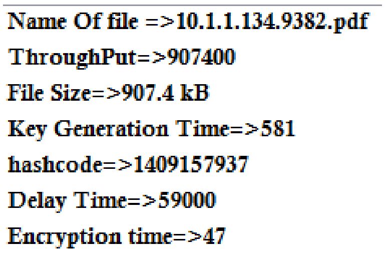
```
run:
run method
From Server: truetrue
From Server: true
From Server: truetrue
From Server: truetrue
From Server: truetrue
From Server: truetrue
```

Figure 6.1: Output to authenticated clients



←T→ ▼	id	fname	lname	fathername	mothername	emailid	dob	password
□ Edit Copy Delete	1	rohit	manhas	tilak raj	naresh	rohitmanhas10@gmail.com	12/05/93	1234567
□ Edit Copy Delete	2	ruytgyu	thg	fhgf	hgf	hgf	hgf	hgf
□ Edit Copy Delete	3	tyt	tyfy	fhg	fghf	ghf	ghf	ghf
□ Edit Copy Delete	4	rt	rr	rr	rgfghf	hfhg	ghfg	fhg
□ Edit Copy Delete	5	rohit	manhas	tilak raj	naresh	rohitmanhas10@gmail.com	12may 1993	12345
□ Edit Copy Delete	6	rohit	manhas	tilak raj	naresh	rohitmanhas10	5may 1993	12345
□ Edit Copy Delete	7	Aashish	Rao	Vijay	Nishi	rao01aashish@gmail.com	24-01-1991	98765
□ Edit Copy Delete	8	ninni	singh	xyz	xyz	eflkfmc	43-939-2222	123321
□ Edit Copy Delete	9	mayank	sharma	kjk	kjk	k	kjkjkjk	mayank
□ Edit Copy Delete	10	Aashish	John Rao	Vijaty Kumar Rao	Nishi Bala Singh	daniel01love@gmail.com	24-01-1991	336321

Figure 6.2: Database entries



```
Name Of file =>10.1.1.134.9382.pdf
ThroughPut=>907400
File Size=>907.4 kB
Key Generation Time=>581
hashcode=>1409157937
Delay Time=>59000
Encryption time=>47
```

Figure 6.3: Factor for measuring performance

the network and can upload his data onto the server or he can download it from there. For every successful upload of data to the server we are provided with the performance metrics mentioned above and they are shown in figure 6.3.

The data stored onto the server is kept in an encrypted form and cannot be downloaded from there, only the client that holds the key to that session is able to access that information, else it will be of no use to it.

Based on the above performance parameters we have shown that our proposed approach yields betters results and is well suited to be implemented in the wireless mesh networks.

In Figure 6.4 we have plotted a graph between the file size in MBs and the time required to generate the keys. Through the graph we can see that the increase in file size is proportional to the time required for generation of keys. The results are better for large file size as they require less time.

In Figure 6.5 the throughput of the network is compared to related file size and the result shows that for the larger file size higher throughput is achieved, therefore this approach is better for large size files even though small size file also gives high throughput.

In Figure 6.6 delay time is being calculated for the various file size and we can see there is not a linear relationship among them as delay could occur due to any random reason in a network such as power down, transmission delay, etc.

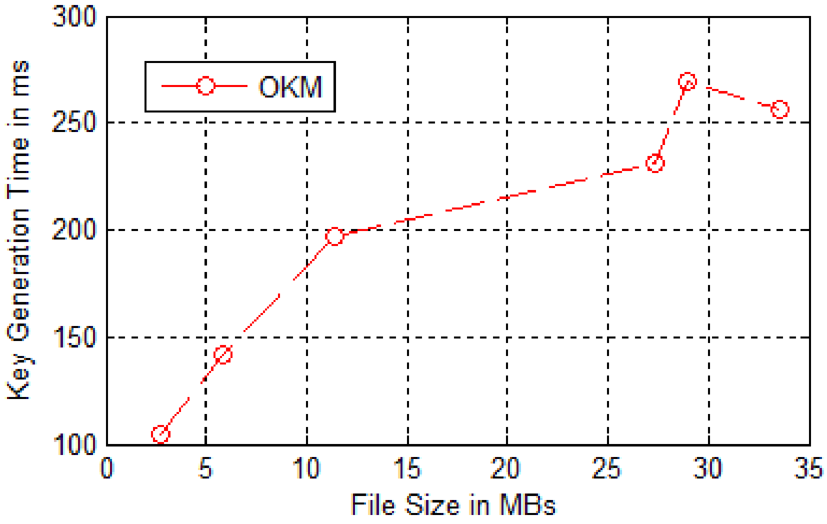


FIGURE 6.4: Key generation time of OKM on different file size in MBs

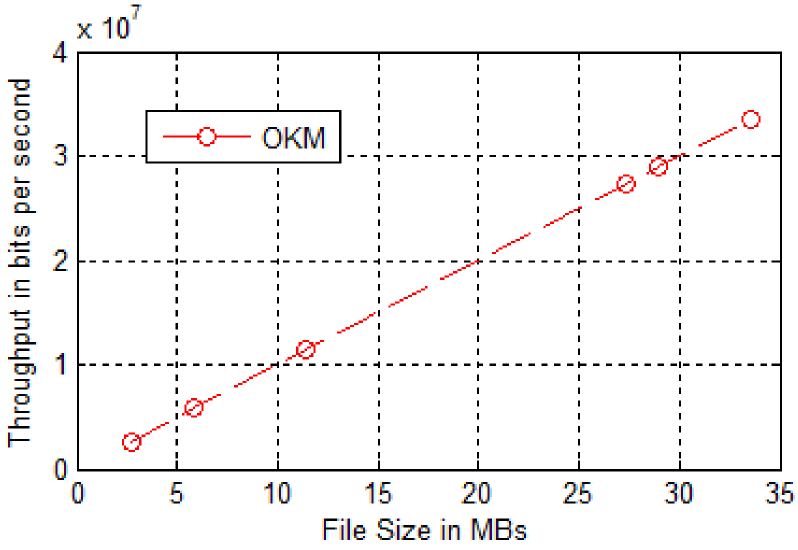


FIGURE 6.5: Throughput on different file size in MBs

While in Figure 6.7 another comparison has been shown between the encryption time of AES and the proposed scheme OKM, the results shows that the prposed key management algorithm provides a better reults for larger file size and is well suited for WMNs.

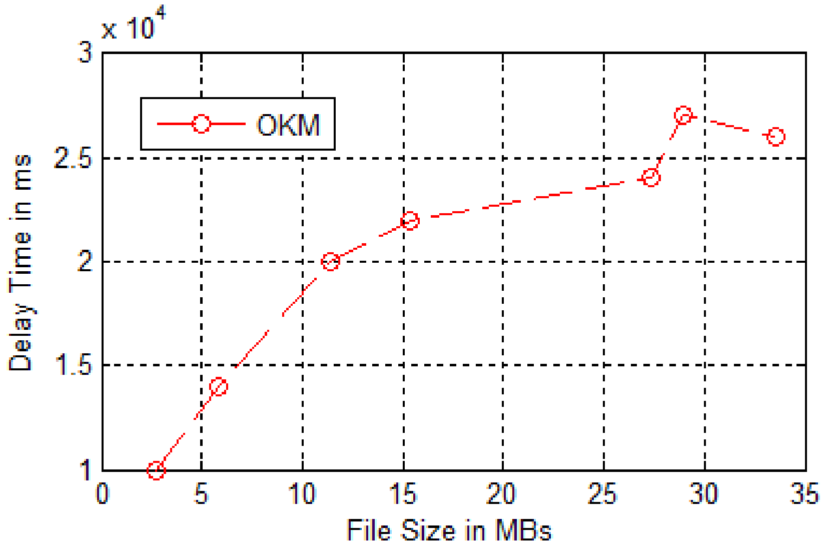


Figure 6.6: Delay time of OKM on different file size in MBs

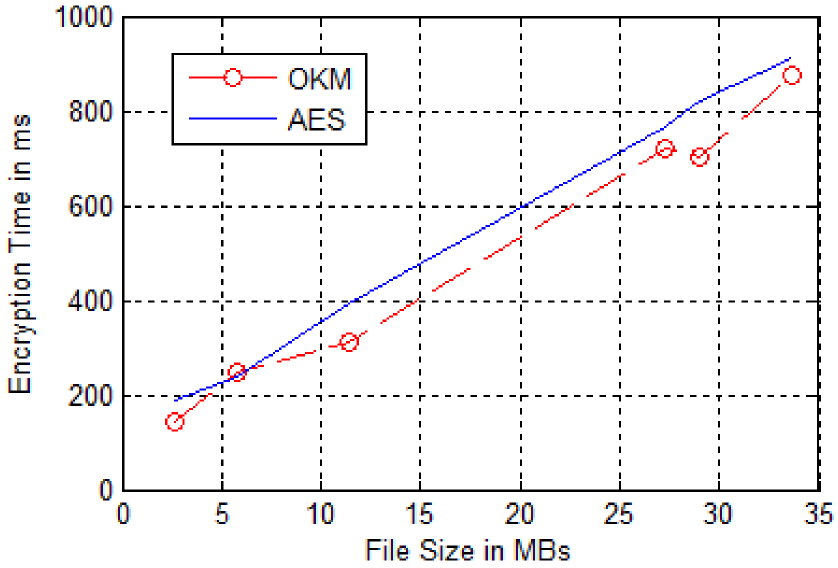


Figure 6.7: Encryption time of OKM and AES on different file size in MBs

CHAPTER 7

CONCLUSION AND FUTURE WORK

7.1 Conclusion

The basic deliverance of key management services in wireless mesh networks is provisioning of security to the users. Due to lack of any trusted authority the existing mechanisms of providing security such as in WiFi, WiMAX, MANET, etc could not be applied to WMNs. If we consider large network sizes and the lack of physical security to the mesh routers then implementation of key management becomes cumbersome in WMNs. Though, in large WMNs, for symmetric key management systems each node is required to pile a large number of keys, due to lack of resources in WMNs many such schemes thus become impractical. In comparison to PKI, it needs fewer number of keys. Signature verification is the most computationally costly process in PKI scheme. Recent developments on pairing based encryption techniques have made it thinkable to use in WMNs. In IBC, the unique ID of a client is used for key generation, thus keys are self-authenticated and the use trusted third-party for delivering the keys makes the network more secure.

In this thesis, we have presented a hybrid key management protocol for WMNs. It associates the pairing based scheme with symmetric key management scheme to propose a better key management protocol for WMNs. Because of the less computational requirements of IBC, in our scheme, we use the IBC based scheme to generate master key based on which our symmetric keys are exchanged. In particular no additional public key information is required, as a consequence very limited messages are exchanged and which leads to less energy consumption. In addition to it, instead of using pre-deployment techniques for computation of keys we are computing the keys only at the time when information is exchanged due to which there is less computation overhead and less storage space is required. Moreover based on the above performance parameters we have shown that our proposed approach is better than previously existing key management techniques and is efficient to be deployed in wireless mesh networks.

7.2 Future Work

Till now, significant amount of work has been done to secure the WMNs. This thesis provides our primary work in this domain. As a very potential research area, there are several motivating future directions:

- Neighbor monitoring to avoid from malicious attacks .
- Develop improved and secure routing protocols to lever multi-hop networks and other issues exclusive to WMNs

BIBLIOGRAPHY

[1] J. Sun, C. Zhang, and Y. Fang, "A security architecture achieving anonymity and traceability in wireless mesh networks," in *INFOCOM 2008. The 27th Conference on Computer Communications.* IEEE, 2008.

[2] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *Network, IEEE,* vol. 13, pp. 24-30, 1999.

[3] A. Egners and U. Meyer, "Wireless mesh network security: state of affairs," in *Local Computer Networks (LCN), 2010 IEEE 35th Conference on*, 2010, pp. 997-1004.

[4] W. Taojun, X. Yuan, and Y. Cui, "Preserving traffic privacy in Wireless Mesh Networks," in *prod of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks* (WoWMoM'06).

[5] J. Sen, P. R. Chowdhury, and I. Sengupta, "A distributed trust mechanism for mobile ad hoc networks," in *Ad Hoc and Ubiquitous Computing, 2006. ISAUHC'06. International Symposium on*, 2006, pp. 62-67.

[6] J. Sen, "A robust and efficient node authentication protocol for mobile ad hoc networks," in *Computational Intelligence, Modelling and Simulation (CIMSiM), 2010 Second International Conference on*, 2010, pp. 476-481.

[7] G. R. Hiertz, D. Denteneer, S. Max, R. Taori, J. Cardona, L. Berlemann, and B. Walke, "IEEE 802.11 s: the WLAN mesh standard," *Wireless Communications, IEEE,* vol. 17, pp. 104-111, 2010.

[8] N. Ben Salem and J.-P. Hubaux, "Securing wireless mesh networks," *Wireless Communications, IEEE*, vol. 13, pp. 50-55, 2006.

[9] Y. Zhang and Y. Fang, "ARSA: an attack-resilient security architecture for multihop wireless mesh networks," *Selected Areas in Communications, IEEE Journal on*, vol. 24, pp. 1916-1928, 2006.

[10] L. Xu and Y. Zhang, "Matrix-based pairwise key establishment for wireless mesh networks," *Future Generation Computer Systems*, vol. 30, pp. 140-145, 2014.

[11] S. Glass, M. Portmann, and V. Muthukkumarasamy, "Securing wireless mesh networks," *Internet Computing, IEEE*, vol. 12, pp. 30-36, 2008.

[12] F. Kandah, W. Zhang, X. Du, and Y. Singh, "A Secure Key Management Scheme in Wireless Mesh Networks," in *Communications (ICC), 2011 IEEE International Conference on*, 2011, pp. 1-5.

[13] Heyun Zheng, Charles R. Barker JR., Surong Zeng, United states patent application publication Pub. No.: US 2007/0147620 A1, Jun. 28, 2007.

[14] F. Martignon, S. Paris, and A. Capone, "MobiSEC: a novel security architecture for wireless mesh networks," in *Proceedings of the 4th ACM symposium on QoS and security for wireless and mobile networks*, 2008, pp. 35-42.

[15] W. Galuba, P. Papadimitratos, M. Poturalski, K. Aberer, Z. Despotovic, and W. Kellerer, "Castor: scalable secure routing for ad hoc networks," in *INFOCOM, 2010 Proceedings IEEE*, 2010, pp. 1-9.

[16] S. Khan, N. A. Alrajeh, and K.-K. Loo, "Secure route selection in wireless mesh networks," *Computer networks*, vol. 56, pp. 491-503, 2012.

[17] A. P. Lauf, R. A. Peters, and W. H. Robinson, "A distributed intrusion detection system for resource-constrained devices in ad-hoc networks," *Ad Hoc Networks*, vol. 8, pp. 253-266, 2010.

[18] C. Pham, "Scheduling randomly-deployed heterogeneous video sensor nodes for reduced intrusion detection time," in *Distributed Computing and Networking, ed: Springer*, 2011, pp. 303-314.

[19] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in *Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on*, 2005, pp. 324-328.

[20] K. Ren, K. Zeng, and W. Lou, "A new approach for random key pre distribution in large scale wireless sensor networks," *Wireless Communications and Mobile Computing, vol. 6*, pp. 307-318, 2006.

[21] A. Mishra and W. A. Arbaugh, "An initial security analysis of the IEEE 802.1 X standard," 2002.

[22] M. Kassab, A. Belghith, J.-M. Bonnin, and S. Sassi, "Fast pre-authentication based on proactive key distribution for 802.11 infrastructure networks," in *Proceedings of the 1st ACM workshop on Wireless multimedia networking and performance modeling*, 2005, pp. 46-53.

[23] A. R. Prasad and H. Wang, "Roaming key based fast handover in WLANs," in *Wireless Communications and Networking Conference, 2005 IEEE*, 2005, pp. 1570-1576.

[24] M. Parthasarathy, "Protocol for carrying authentication and network access (PANA) threat analysis and security requirements," 2005.

[25] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "LHAP: a lightweight hop-by-hop authentication protocol for ad-hoc networks," in *Distributed Computing Systems Workshops, 2003. Proceedings. 23rd International Conference on*, 2003, pp. 749-755.

[26] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "LHAP: a lightweight network access control protocol for ad hoc networks," *Ad Hoc Networks*, vol. 4, pp. 567-585, 2006.

[27] H. Moustafa, "Providing authentication, trust, and privacy in wireless mesh networks," *book chapter in: Security in Wireless Mesh Networks. Y. Zhang et al.(eds.)*, pp. 261-295, 2007.

[28] B. Lai, S. Kim, and I. Verbauwhede, "Scalable session key construction protocol for wireless sensor networks," in *IEEE Workshop on Large Scale RealTime and Embedded Systems (LARTES)*, 2002, p. 7.

[29] H. Chan and A. Perrig, "PIKE: Peer intermediaries for key establishment in sensor networks," in *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, 2005, pp. 524-535.

[30] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Security and Privacy, 2003. Proceedings. 2003 Symposium on*, 2003, pp. 197-213.

[31] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: a survey," *Communications Surveys & Tutorials, IEEE*, vol. 11, pp. 52-73, 2009.

[32] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *SIAM Journal on Computing*, vol. 32, pp. 586-615, 2003.

[33] L. Martin, *Introduction to identity-based encryption*: Artech house, 2008.

[34] S. William and W. Stallings, *Cryptography and Network Security, 4/E*: Pearson Education India, 2006.

[35] W. Diffie and M. E. Hellman, "Special feature exhaustive cryptanalysis of the NBS data encryption standard," *Computer*, vol. 10, pp. 74-84, 1977.