Wireless Personal Communications (2020) 114:3457–3475
https://doi.org/10.1007/s11277-020-07541-6

An Attack Resilient Framework in Cognitive Radio Network Environment for Inter-domain and Intra-domain Communication

Geetanjali Rathee[1] · Naveen Jaglan[2] · Binod Kumar Kanaujia[3]

Published online: 6 June 2020

Abstract

In this manuscript, we have considered the number of security concerns at different aspects of network communication in hybrid (centralized or distributed) cognitive radio network cell environment by distributing it into inter-domain and intra-domain. We have identified and resolved the routing and handoff process threats in both the domains by proposing a secure communication framework. The intra-domain security threats include routing and handoff CU attacks that are firmed by a Trust Analyzer which computes the TV/TF of each transmitting node or CU. Further, the inter-domain security mechanism efficiently recognized the malicious behavior of the handoff CU during real time communication by proposing a ticket based mechanism. For this, an authentication server is liable for generating and distributing the tickets to all the handoff users by verifying their authenticity. The proposed framework is validated against conventional security mechanism over certain networking parameters such as network throughput, packet delivery ratio, packet loss ratio, falsification attack, average authentication, maximum authentication and probabilistic scenarios of authentication mechanism for both the domains.

Keywords Cognitive radio network · Secure CRN · Trusted CRN framework · Trust value · Authentication · Probabilistic authentication scenarios

✉ Geetanjali Rathee
geetanjali.rathee123@gmail.com

Naveen Jaglan
naveenjaglan1@gmail.com

Binod Kumar Kanaujia
bkkanaujia@ieee.org

[1] Department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat 173234, India

[2] Department of Electronics and Communication Engineering, Jaypee University of Information Technology, Waknaghat 173234, India

[3] School of Computational and Integrative Sciences, Jawaharlal Nehru University, New Mehrauli Road, New Delhi 110067, India

1 Introduction

The continuous declination in communication cost has leaded the business tasks organizations to be heavily dependent on the wireless networking technologies in order to stake the information in an effective and creative manner. Further, the expansion in wireless technologies has endorsed the societies to use the network not only to stake the resources but also to accumulate large pool of data for scrutiny [1]. However, the emergence and advancement of new wireless deployments has resulted in increased demand for spectrum availability [2]. Because of increased spectrum requirements, the spectrum usage measurements in various countries have revealed the issue of spectrum scarcity. However, in order to overcome this issue, Cognitive Radio (CR) technique has been introduced to allow the secondary/Cognitive Users (CUs) to use the idle channels of Primary Users (PUs) as depicted in Fig. 1. The spectrum sensing, decision, sharing (access) and handoff or mobility are the following phases performed by CR technology using cognitive engines to occupy the idle spectrum band released by the PU transmitter [3]. In the first three phases of CR cycle, the CU sanities the environment to distinguish the idle channel and choose the most operative unused band amongst all channels. Further, it inaugurates the communication on the selected channel via suitable retrieving strategy in order to avoid meddling between the PU and several CUs [4]. However in the last function of CR engine, the CU desires to switch its current transmission on another accessible channel with the emergence of PU during data transmission. Further, the continuous advancements in wireless technologies pose a big challenge to the security of organizations' resources [5]. The risk of threats increases as the communication between the CU's (within a range known as intra-domain or outside the range of a particular base station where it needs to connect to another base

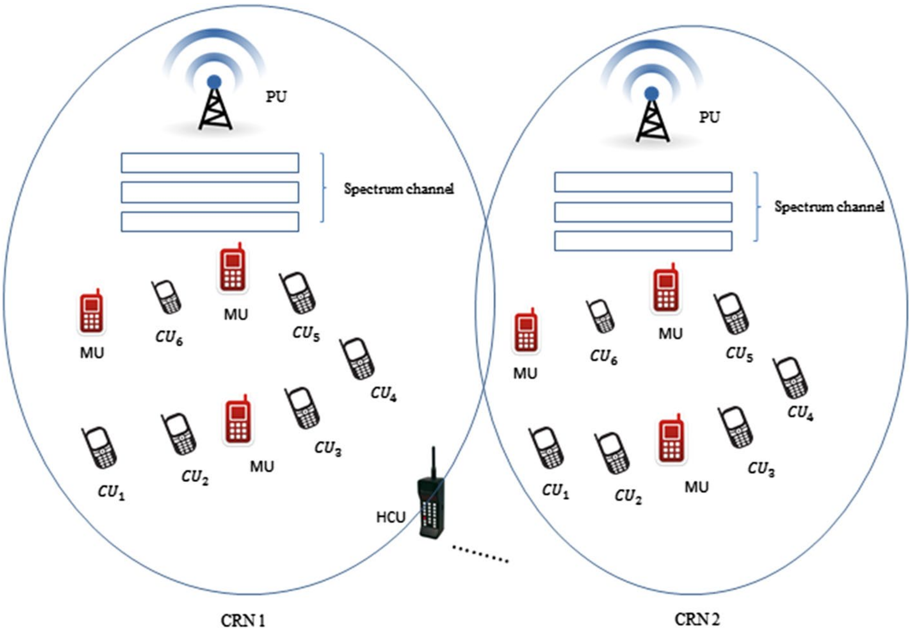


Fig. 1 Cognitive radio network environment

station known as inter-domain) is processed. During the handoff process within (intra) or between (inter) the domains, the mobile CU leaves the range of its current base station and connects with a Foreign Base Station (FBS) in another network's domain to endure its networking services. In order to access the services, the handoff cognitive user (HCU) desires to authenticate itself with the FBS [6]. However, during the communication process in both the domains, there is a possibility to encounter a Malicious User (MU) which may try to communicate with the FBS by forging the identity (id) of legitimate HCU or imitating itself as a trusted HCU [7, 8]. Further, from the security perspective, it is possible even within a domain (intra-domain) where a MU imitate the legitimate HCU, new cognitive user (NCU) and Transmitting Nodes (TNs) through which data is communicated among the CU's can be compromised with the intention to degrade the overall network performance. In practice, the CUs can be compromised by the intruders to introduce malicious threats in the cognitive radio network cell (CRNC) environment [9] and the compromised CU behaves as a MU. Further, NCU may encounter as a MU that remains silent in network for long period of time and then after recognizing other nodes pattern may try never allow the legitimate CU to access the channel by repeatedly behaving as a trusted HCU to further significantly affect the network security [10]. Thus, the potential challenge of HCU is to get distinguished from the MU in order to establish a trusted handoff mechanism.

Moreover, as the possibility of threats exists at almost each layer of the communication process such as from the channel allocation process to the handoff and message transmission phenomenon, there is a need to establish a secure communication mechanism in the network. In this manuscript, we have discussed a number of security threats at two different aspects which are (1) attack on message TNs, HCUs during intra-domain communication and (2) attack on HCU during inter-domain communication. In former, where CU's accesses their network services through TNs, there may be a possibility where either TN acts maliciously or CU's are compromised to behave maliciously with the aim of degrading the network metrics [11–13]. Further, upon emergence of PU, the current communicating CU needs to vacate the channel and handoff to another ideal channel. Now, during the handoff, a MU behaves as a legitimate HCU or a New User (NU) may encountered as MU in order stop accessing the network services of ideal HCU [14, 15]. In latter, during the handoff of CU that accesses the services in real time scenarios, the MU may trace the moving pattern of legitimate HCU or simply forge their ID's for further stopping the communication process. To resolve all the discussed issues at different stages of communication process, researchers/scientists have proposed a number of security strategies. However, none of the researchers have focused on the CRN to provide the HCU security in both the domains. The purpose of this paper is to provide a secure CRN by proposing a number of security frameworks. The potential contribution of the paper is systematized as follows.

- Ensuring the security upon accessing the network services to TNs, CUs, NCUs or HCUs in inter-domain and intra-domain communication.
- The approach is validated through NS2 simulation against conventional security approach by measuring the network throughput, packet delivery ratio, packet loss ratio, falsification attack, average authentication, maximum authentication and probabilistic scenarios of authentication mechanism.

The remaining organization of the paper is structured as follow. The related works of security techniques at certain stages of CRN are presented in Sect. 2. The network model of the proposed mechanism is discussed in Sect. 3. Further, in Sect. 4, the security framework along with various attacking strategies has been proposed at different aspects of communication process. Moreover the numerical analyses of the proposed mechanism over certain performance metrics are discussed in Sect. 5. Lastly, Sect. 6 concludes the work and highlights the future scope.

2 Related Work

In this section, we have discussed various security frameworks or techniques proposed by different author's. Several security techniques such as secure routing or handoff frameworks/mechanisms/protocols have been proposed by various scientists. Chen et al. [16] have projected a joint spectrum sensing and resource allocation (JSSRA) scheme in CRN to incentive CUs to behave well. A lagrangian dual and brute force algorithms are formulated to optimize the resource allocation and cooperative CUs decision problems. The proposed mechanism improves the system robustness during cooperative decision and its utility gain in resource allocation. Further Althunibat et al. [17] have proposed a novel attacker-identification and attacker-punished algorithms to detect and punish the attackers either by leaving the network or to sends false results. The algorithm relies on delivery-based assessment strategies where the transmitted data is evaluated to made the individual reports and take a global decision. The proposed algorithm successfully enhances the performance in case of large number of attackers. Further, a peer-predict method is proposed by Gan et al. [18] to identify the MU's. To punish or to identify the MUs, the incentivize CUs sends the truthful reports simultaneously for taking the decision fusions. The proposed algorithm rewarded the trusted CUs for sending truthful results and penalty the MU for making the false reports. A significant improvement is made over detection rates when more than half MU conducts SSDF attack. Moreover, Vosoughi et al. [19] have offered a consensus-based iterative scheme to reduce the spectrum efficiency and increases interfere with the PUs where the trust management scheme is provided to mitigate the SSSDF attack in terms of false alarm and miss detection error rates. Further, the authors in [20–22] have proposed several security techniques against routing threats. Liu et al. [20] suggested a forwarding assessment based detection (FADE) scheme by focusing on DOS called as grey hole attack. FADE scheme detects the collaborative grey hole attacks by monitoring 2-hop acknowledgement phenomenon. The performance investigation of the proposed mechanism is analyzed over sum of positive false rate and negative false rates. Li et al. [21] offered an ad-hoc on demand reliable path distance vector mechanism for MANETs where the protocol discovers multiple loop-free paths by evaluating the different aspects i.e. trust values and hop counts. The experimental results of the proposed mechanism improve the packet delivery ratio (PDR) from grey hole, black hole and packet alteration attacks. Further Liu et al. [22] have proposed an active trust approach based on trust routing scheme and active detection-based security. The proposed mechanism efficiency avoids the black hole attack using active creation of nodal trust. The active nodal trust provides better data route security over black hole attacks in comparison of previous studies. Maximum of the researchers have resolved the grey/black hole routing threats by computing the trust value of the nodes. Although a number of trusted mechanisms have been suggested in MANETs, mesh network or sensor networks, however, none of the security techniques have been imported on CRN environment. Furthermore, the numbers of handoff security mechanisms [23–25] have been proposed using cryptographic techniques or trust based mechanisms.

In this paper, we would like to propose a secure communication process in CRNC environment by focusing on routing and handoff processes attacks. In the routing phenomenon, a trust based routing mechanism is proposed which has been proposed for MANETs and WSNs and cannot be adoptable yet in CRNs. In this paper, the author's aim is to propose a trust based mechanism of identifying the legitimate CU's during the message transmission in CRNC environment. Further, although a number of cryptographic techniques have been proposed by various scientists, however, these techniques cannot be feasible in CRN environment because of its larger storage, communication and computation overheads. In order to overwhelm the above disputes, a ticket based handoff technique is proposed for authenticating the HCU in the CRN. At last, all these security techniques have been merged into CRNC environment in both the domains to analyze the feasibility of the entire network.

3 Network Model

This section describes the network model of the proposed framework for ensuring the TNs and handoff security during intra-domain or inter-domain communication. The proposed system model is a hybrid CRN environment as depicted in Fig. 2 i.e. centralized network

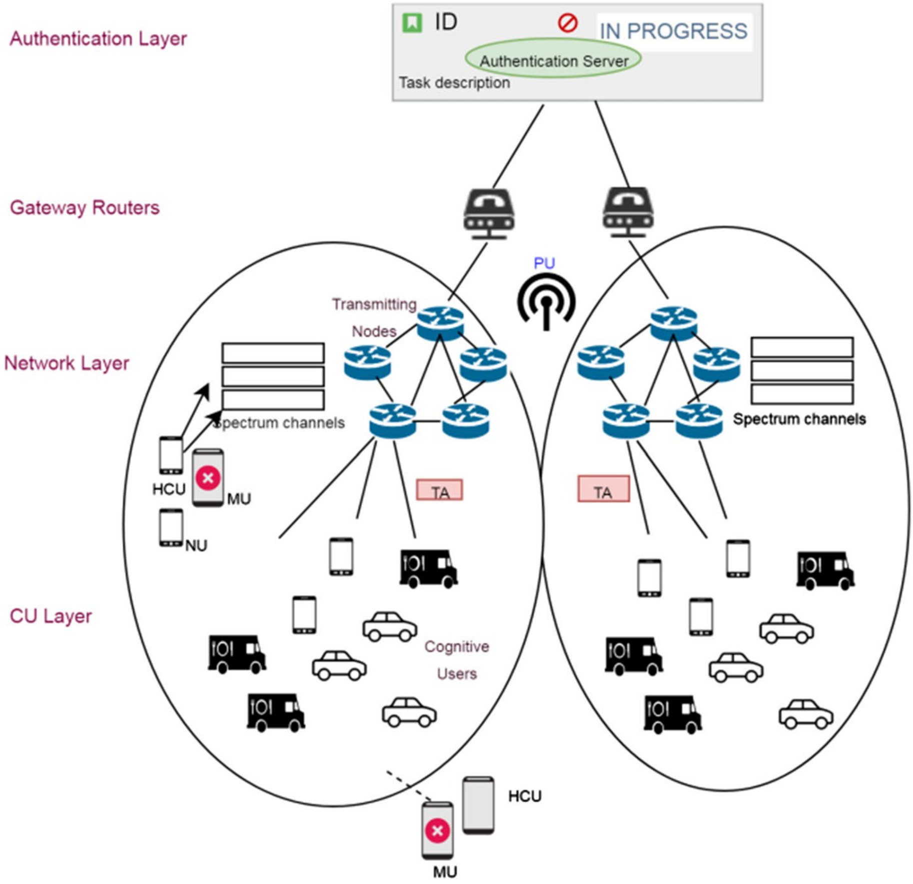


Fig. 2 Proposed security framework network model

because of single authentication server (AS) and distributed network because of number of Domain Controlling units (DCU) and a coordinator i.e. Trust Analyzer (TA). The AS located at the top layer that includes various domains of cognitive network and is responsible for ensuring the security to the HCU by generating, distributing and periodically updating the tickets ‘T’ between the domains. While, the trusted internet gateway routers (IGRs) which act as backbone provide the connectivity between the AS and the network domains (NDs) to ensure the legitimate transmission of messages.

Further, the TA is responsible for providing the intra-domain communication including TNs’, CUs’ and HCUs’ security. Each ND includes N_{CU} number of CU which access the network services, N_R number of routers (R) through which the services are provided and a TA having MR functionalities that is responsible to receive the idle channel information from the PUs and to allocate requested channels to the corresponding CUs.

4 Proposed Trusted or Secure Framework

In this section we have discussed the number of attacking strategies at CUs, NCUs or HCUs along with their detection and removing phenomenon in both the domains in detail.

(a) Trusted Security Framework for Intra-domain Communication

The principle of proposing the security framework within a domain is to detect and resolve the malicious activities of TN at Network Layer (NL) and CUs and HCUs or NUs at CU layer by defining a TA as presented in Fig. 2. It is a controlling unit of the NL and CU layer that is responsible for verifying the legitimacy of CU, NU or HCU within the domain. In order to ensure the security during message communication, a trusted routing framework is proposed by computing the TV/TF of each layer. An analytical description of the proposed framework has been presented in this section by categorizing the approach into two different cases which are: (1) when the TN is identified as Malicious Node (MN) and (2) when the Malicious User (MU) is identified during the handoff of CU or upon the emergence of New User (NU). The proposed security framework’s aim is to resolve the identified MNs or MUs by computing the TV/TF of all CUs, NUs and HCUs in CRN. The system model of the proposed framework is depicted in Fig. 2 comprising a decentralized CU environment including TA and n number of TNs among which some are elected as MNs. Similarly, CU layer consist of TA, n number of CUs among which some are selected as MUs, NUs and HCUs. The TN’s are fixed while CUs are mobile where users may move from one place to another or a new user may enter anytime anywhere in the environment. Initially, during the network establishment, all the nodes are assumed to be trusted and legitimate. However, the threat of security increases with the increase in communication process between the nodes. The flowchart of the proposed intra-domain secure mechanism is depicted in Fig. 3. In order to measure the authenticity of the proposed framework, numbers of MNs or MUs are randomly deployed in the NL and CU layer upon the entry of NU or during handoff process. The intent of MN or MU is to decrease the performance of the network by restricting the trusted CUs to access the network services. In the proposed framework, the TA keeps the record of TV including CU_i, CU_{addr}, HCU_{st}, TV_i, MU_i, CU_i, CU_{addr}, $TV_{i,} andMN_i$ into its look up table. The TV of TNs depends upon the DDR and liveliness of the communicating nodes while CU’s TV is computed by checking the Survival Time (ST), previous history interaction and request services of the CUs. Whenever, a NU

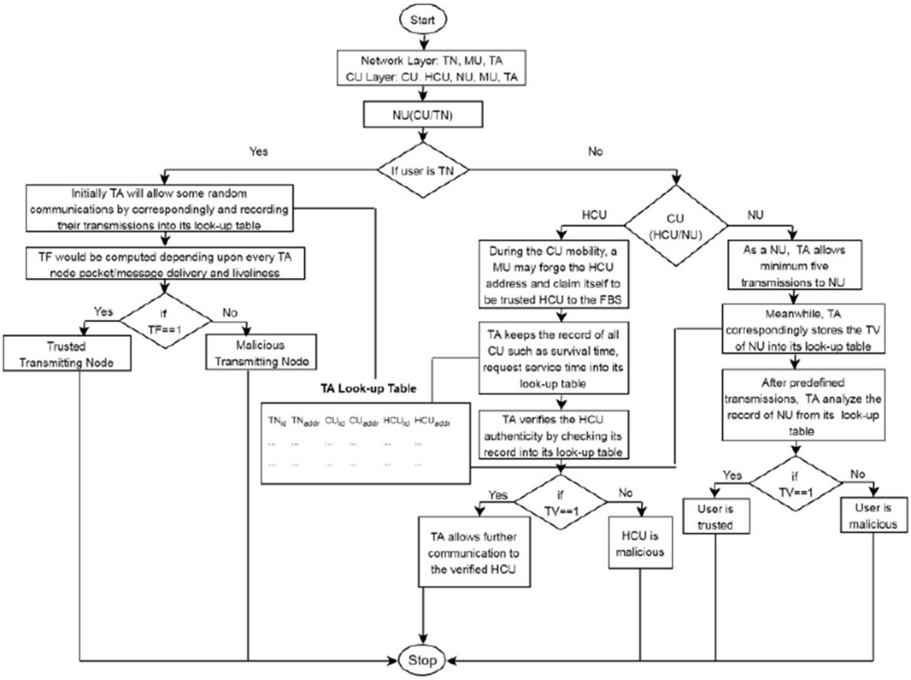
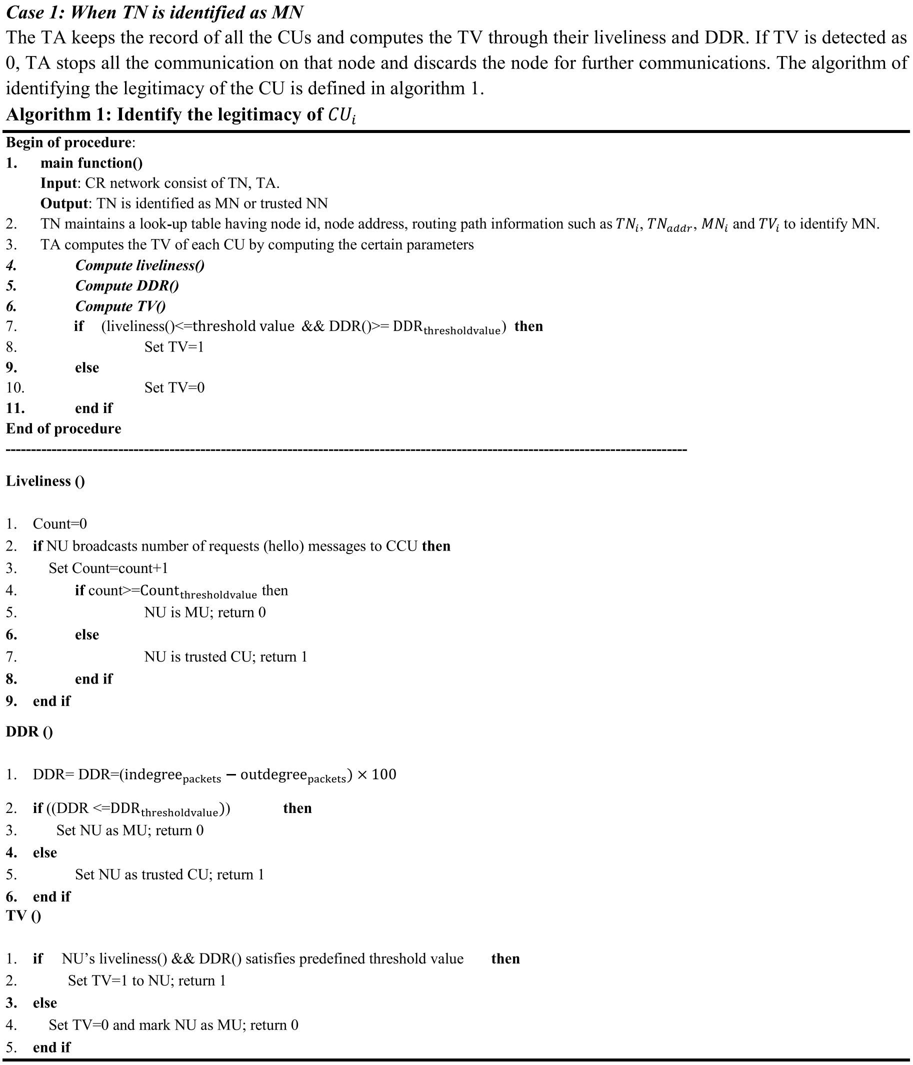

Start
Network Layer: TN, MU, TA
CU Layer: CU, HCU, NU, MU, TA
NU(CU/TN)
Yes
If user is TN
No
Initially TA will allow some random communications by correspondingly and recording their transmissions into its look-up table
TF would be computed depending upon every TA node packet/message delivery and liveliness
Yes
if TF==1
No
Trusted Transmitting Node
Malicious Transmitting Node
TA Look-up Table
TN_{id} TN_{addr} CU_{id} CU_{addr} HCU_{id} HCU_{addr}
HCU
CU (HCU/NU)
NU
During the CU mobility, a MU may forgo the HCU address and claim itself to be trusted HCU to the FBS
TA keeps the record of all CU such as survival time, request service time into its look-up table
TA verifies the HCU authenticity by checking its record into its look-up table
Yes
if TV==1
No
TA allows further communication to the verified HCU
HCU is malicious
As a NU, TA allows minimum five transmissions to NU
Meanwhile, TA correspondingly stores the TV of NU into its look-up table
After predefined transmissions, TA analyze the record of NU from its look-up table
Yes
if TV==1
No
User is trusted
User is malicious
Stop

Fig. 3 Proposed framework to check the legitimacy of HCU for intra-domain communication

enters into CU layer, the initial step of TA is to identify whether the user is HCU or NU by checking its look-up table. If the user is identified as NU, TA allows some initial transmission and keeps the record of its activity into its look up table.

However, in case when CU is identified as HCU, TA judges the legitimacy by checking its request services, ST and previous history interactions. The detailed explanation of both the layers is elaborated in further texts using different cases.

Case 1: When TN is identified as MN The TA keeps the record of all the CUs and computes the TV through their liveliness and DDR. If TV is detected as 0, TA stops all the communication on that node and discards the node for further communications. The algorithm of identifying the legitimacy of the CU is defined in Algorithm 1.



Case 1: When TN is identified as MN

The TA keeps the record of all the CUs and computes the TV through their liveliness and DDR. If TV is detected as 0, TA stops all the communication on that node and discards the node for further communications. The algorithm of identifying the legitimacy of the CU is defined in algorithm 1.

Algorithm 1: Identify the legitimacy of CU_i

```
Begin of procedure:
main function()
Input: CR network consist of TN, TA.
Output: TN is identified as MN or trusted NN
TN maintains a look-up table having node id, node address, routing path information such as $TN_i$, $TN_{addr}$, $MN_i$ and $TV_i$ to identify MN.
TA computes the TV of each CU by computing the certain parameters
    Compute liveliness()
    Compute DDR()
    Compute TV()
    if (liveliness()<=threshold value && DDR()>= $DDR_{thresholdvalue}$) then
        Set TV=1
    else
        Set TV=0
    end if
End of procedure
--------------------------------------------------------------------------------

Liveliness ()

Count=0
if NU broadcasts number of requests (hello) messages to CCU then
  Set Count=count+1
    if count>=$Count_{thresholdvalue}$ then
        NU is MU; return 0
    else
        NU is trusted CU; return 1
    end if
end if

DDR ()

DDR= DDR=$(indegree_{packets} - outdegree_{packets}) \times 100$
if (($DDR <= DDR_{thresholdvalue}$)) then
   Set NU as MU; return 0
else
    Set NU as trusted CU; return 1
end if

TV ()

if NU's liveliness() && DDR() satisfies predefined threshold value then
    Set TV=1 to NU; return 1
else
  Set TV=0 and mark NU as MU; return 0
end if
```

*Case 2: When NU or HEU is identified as MU*The TA computes the TV of all the CUs, NUs or HCUs by checking the request services, ST and previous history interactions. In the CU layer, there are two possibilities, whether the CU is HCU or NU. If it is HCU, then there is the possibility to encounter the attack and upon the handoff of CU, there are two kinds of possibilities.

The first possibility is when MU enters randomly and behaves like a legitimate HEU and requests the TA to access the services In that case, the TA needs to check the look up table in order to know the CU's id along with its previous history interactions, ST and number of request messages (RM). The legitimate HCU has older time and done less number of RM as compared to that of MU and has also done some transmissions T inside the network. Therefore, the HCU identifies the user as legitimate EU and allows the further services access to HCU as follows:

$$HCU = \begin{cases} CU\ :\ ST_{CU} > ST_{CU}, RM_{CU} > RM_{MU} and\ have\ some\ transmission\ T \\ MU\ :\ ST_{CU} > ST_{MU}, RM_{CU} > RM_{MU} and\ have\ no\ transmission\ T \end{cases}$$

The CU's TV is computed by verifying the certain characters of the user such as RM, AT and TV. The service RM identifies the malicious behavior by checking the number of broadcast requests sends to the CU. The MU sends a lot of service RM (assumed more than 10 requests/millisecond as threshold value) to the TA for insisting the requested channel. Further, the AT is considered to be an important parameter to measure the malicious behavior of the user. The MU's AT is always less than the existing CU and history interactions would be 0 or very less. Depending upon these factors, the TV of each user would be computed either 0 or 1. If service RM and AT character satisfies a predefined threshold value, then TV will be 1 else 0.

In another case, where the NU is identified as NU, the possibility of cases can be raised as:

$$NU = \begin{cases} CU \\ MU \end{cases}$$

Now, as the AT and previous history interaction of NU is very less as compared to that of the existing CU, hence initially, the TA allows at least 15 communication transmissions to the NU (as per assumptions). If the NCU is CU then TV of CU would be trusted and satisfied by the threshold value and if the NCU is MU, TV would always be below the predefined threshold range (i.e. 0). The CU keeps the record and transmission information of all CUs in its look up table and after the specified number of transmission, the TV of NCU would be checked by CU and takes the corresponding action against the MU.

$$NU = \begin{cases} (TV == 1) thenCU \\ (TV == 0) thenMU \end{cases}$$

If TV of NU is 1, then user is identified as trusted CU and would allow the further requests transmission else it will simply block all the further requests of NU by considering it as MU.

Algorithm 2: Complete Execution of Proposed Mechanism

```
Assumptions: $\text{Count}_{\text{thresholdvalue}} = 55\%$ and $\text{DDR}_{\text{thresholdvalue}} = 75\%$.
main function()
Input: CU Layer consist of TA, MU, $N$ number of CUs among which one is elected as MU.
Output: HCU or NU is identified as MU or trusted
TA maintains a look-up table having user id, user address, routing path information such as $HCU_{id}$, $CU_{id}$, ST and TV of each user to identify MU.
while ( NCU is HCU)
    Compute ST ()
    Compute RM()
    Compute TV()
    if (ST()<=threshold value && RM()>= $\text{RM}_{\text{thresholdvalue}}$) then
        Set TV=1
    else
        Set TV=0
    end if
Else (NU is CU)
    NCU allow fifteen transmissions
    Record the TV of NU by computing ST() and RM()
    if TV=1 then
        Allow further transmissions
    else
        User is elected as MU
    end if
```

```
Survival Time ()
Count=0
if NU broadcasts number of requests (hello) messages to NCU then
    Set Count=count+1
        if count>=$\text{Count}_{\text{thresholdvalue}}$ then
            NU is MU
        else
            NU is trusted CU
        end if
end if
```

```
RM ()
RM= $\text{RM}(\text{indegree}_{\text{packets}} - \text{outdegree}_{\text{packets}}) \times 100$
if ((RM <=$\text{RM}_{\text{thresholdvalue}}$)) then
    Set NU as MN
else
    Set NU as trusted CU
end if
```

```
TV ()
if NU's ST() && RM() satisfies predefined threshold value then
    Set TV=1 to NU
else
    Set TV=0 and mark NU as MN
end if
```

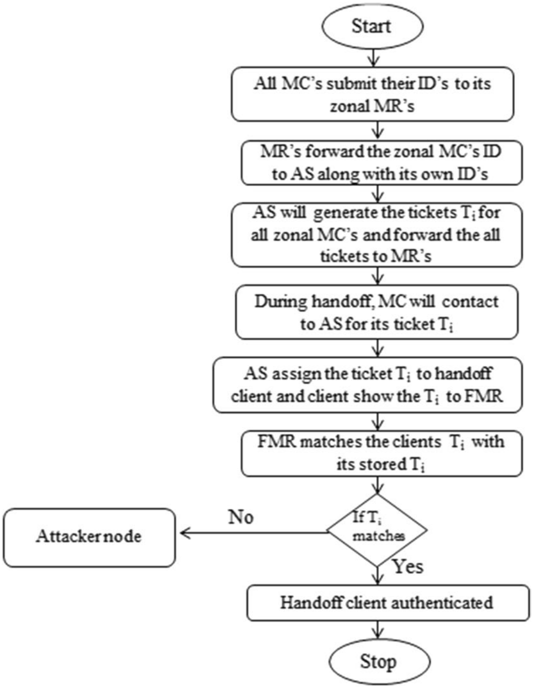
(b) Attack at HCU during Inter-domain Communication

Initially, each CU in the ND senses its network environment in edict to perceive the conduits status and reports to the TA with this information using the control channel which is expected to be always available. Each CU requests for an idle spectrum channel from the TA to start its communication. Whenever, a CU wants to communicate with another CU or wishes to access the network services then the communication between CUs will be done via multiple routers where each router will submit its id along with its CU's id to the AS. The AS will generate the ticket 'T' consisting of $CU_{id}, router_{id}, destination_{id}, expirationtime(et)andanounce(\eta)$ corresponding to each CU and send all the domains' CUs tickets to the routers for ensuring the security and forward to the HCU upon request. Now, let a HCU moves from one ND to another ND then it will contact to the AS via multiple routers for accessing the ticket ‘T’. After accessing the ticket ‘T’, HCU will move and requests the AS to continue its further communication by proving its authenticity to its ranging FBS. The FBS will take out the ticket of particular HCU from its database and correspondingly ask for the ticket ‘T’ from the HCU which will allow the further communication only after verifying both the tickets.

$$\left\{ \begin{array}{c} if\left(ticket_{FBS} == ticket_{HCU}\right) then\ cognitive\ user\ is\ trusted\ else \\ the\ user\ is\ malicious \end{array} \right.$$

As there is possibility of networking attacks being encountered at almost each stage of the communication process, therefore, in the proposed mechanism, we have discussed the security threats at two different aspects during handoff in inter-domain communication in real time scenarios. The flowchart of the mechanism is depicted in Fig. 4. During handoff communication, where HCU send its ticket ‘T’ to the FBS for proving its legitimacy, there is a possibility that a MU forges the id and behave as a legitimate HCU by showing the random generated ticket T to the FBS. In order to overcome this issue, the proposed mechanism contains the following attributes in the ticket T such as $\mathrm{CU_{id}}$, $\mathrm{router_{id}}$, $\mathrm{destination_{id}}$, expiration time (et)and a nounce (η). The first attribute $\mathrm{CU_{id}}$ is the ‘id’ of the HCU which will be verified by the FBS during handoff authenticity. Further, et and η are used to distinguish between the trusted and malicious HCU if a malicious user forges the ticket of a legitimate HCU and show to the FBS after waiting for random number of times then the ticket of that HCU would be expired. The reason is as because AS updates the tickets of all the CUs by periodically locating their locations. Similarly the nonce η is a keyword which will be known by the legitimate HCUs so that even if the MU generates any random ticket T then it will not be verified because of its missing nonce η.

Fig. 4 Secure handoff mechanism for inter-domain communication


Start
All MC’s submit their ID’s to its zonal MR’s
MR’s forward the zonal MC’s ID to AS along with its own ID’s
AS will generate the tickets Tᵢ for all zonal MC’s and forward the all tickets to MR’s
During handoff, MC will contact to AS for its ticket Tᵢ
AS assign the ticket Tᵢ to handoff client and client show the Tᵢ to FMR
FMR matches the clients Tᵢ with its stored Tᵢ
If Tᵢ matches
No
Attacker node
Yes
Handoff client authenticated
Stop

The algorithm of the proposed mechanism is presented below by considering all the attacks with their overcoming strategies.

Input: The network consist of an AS, IGRs, n number of NDs where each ND includes a DCU, a MU, N_R number of mesh routers, N_{CU} number of cognitive users (CU) among which one is elected as HCU.

Output: The CU is identified as trusted CU or MU.

Assumptions

1. An AODV routing mechanism is used to direct the data packets.
2. AS generates the ticket T having$CU_{id}, router_{id}, destination_{id}, expiration\ time\ (et) and\ a\ \ nounce\ (\eta)$. Corresponding to all NDs cognitive users.

```
Main function ()
Step 1 // During message transmission
    If $CU_i$ wants to communicate with $CU_j$then
        CU will request for an idle channel from TA and will start the communication.
    The communication between $CU_i$ and $CU_j$ is done via multiple routers$N_R$
    To identify the legitimacy of routed paths
    Compute DDR()
    If intermediate DDR() satisfies threshold value then
    Continue communication
    Else
    Compute another path
    End If
    End If
Step 2 // During handoff authenticity
    If CU move from $ND_i$ to $ND_j$then
    Compute HCU()
    If ($ticket_{FBS} == ticket_{HCU}$) then
    Provide network services
    Else
    Stop communication
    End If
    End If
```

```
Compute DDR ()
    Each  intermediate router will compute the DDR of its preceding node given as:
        $DDR = \frac{packets\ received\ by\ current\ router}{packets\ recieved\ by\ preceding\ router}$
    If (DDR satisfies threshold value) then
    Router is trusted
    Else
        Current router will send an alarm message to its 2-hop prior router to intimate its succeeding router is malicious.
    End If
```

```
Authenticity HCU ()
    Each NR routers will submit their zonal  $N_{CU}$ id along with their id to the AS.
    AS will generate ticket T of all $N_{CU}$to all zonal routers.
    If a CU move from one ND to another ND then
    HCU will request for its ticket T to show to FR from AS
    AS will send ticket T of HCU through multiple routers.
    HCU will send the ticket T to FR for legitimacy
    FR has the tickets of all CUs and will verify the ticket T of particular HCU from its database
    If $ticket_{FBS} == ticket_{HCU}$then
    HCU is legitimate and allow further communications
    Else
    Stop all the communications
    End If
    End if
```

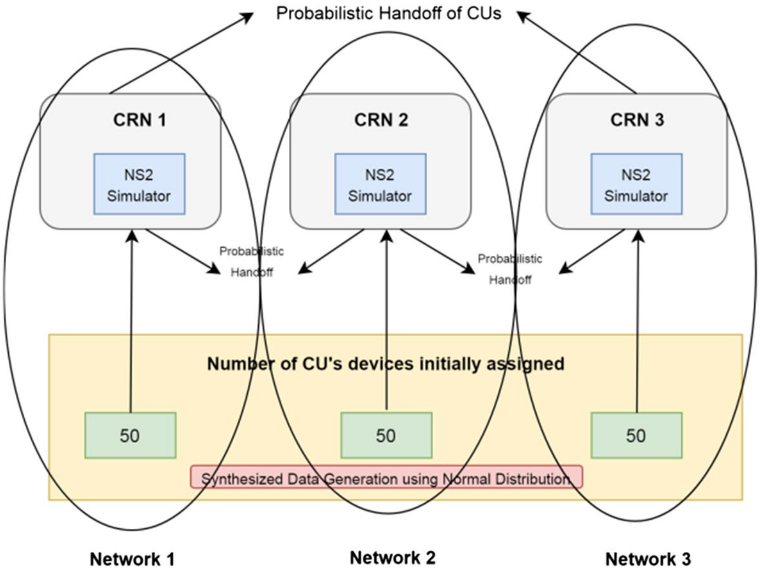


Fig. 5 Test bed of proposed framework for performance analysis

Table 1 Simulation parameters

Number of nodes in a CRN	25, 250
Grid facet	600 m × 600 m
Transmission Range	140 m (approx.)
Data Size	512 Bytes
Simulation time	80 S
Physical Layer	PHY 802.11

5 Performance Evaluation

Although it is a challenging problem to ensure the security at network and CU layer at once, however, we have presented a trusted security framework that not only ensures the high level trust between the nodes but also provide the network services to the cognitive user's that are legitimate. Figure 5 presents the abstracted view of test bed with major components and links. Three CRN are running a version of NS2 with pre-defined number of CU's. The NS2 is running three CRN environments. As presented in Table 1, a 600 m × 600 m network area is constructed having small and large network sizes consisting of 25 and 250 number of nodes respectively. The CUs are portable in nature that is they can abscond their network and join the other network vary at any time and the mobility rate of CU is fixed as 0–10 m/s with the communication sort of 30 m/s. Further, the MAC layer protocol used is 802.11 and transmission ranges of MAP routers are 120 m/s. An initial random TV has also been assigned to each node. Initially, 50 nodes are created that act as IoT devices. Further, a synthetic data generator is worn that generated the data using normal distribution pattern. In order to measure the security, the malicious nodes or CU's are added into the environment based on probability distribution during communication and handoff process. Black hole and worm hole are taken as severe routing attacks because

Table 2 Configuration of NS2 for different CRN environment

S. No.	Virtual machine	Transmitting nodes	Cognitive nodes	Levels
1	CRN 1	25	15	20
2	CRN 2	150	30	40
3	CRN 3	250	50	60

Table 3 Different probabilities used for performance analysis of proposed framework

S. No.	Activity	Probability (%)
1	Addition of malicious node	20
2	Handoff nodes	15
3	Conversion to malicious during handoff	15

the former threat drastically affect the network performance by dropping the 100% of data packets while latter selectively drop the packets and cannot be recognized too soon. Handoff process occurs when any IoT device switches from one CRN to another upon emergence of PU. Addition of malicious node, handoff CU's and conversion of CU to malicious CU is based on probability listed in Table 2 that is out of 250 deployed IoT devices and NN 20 are malicious. The handoff probability signifies that on single unit of time 5 out of 50 or 10 out of 100 nodes change their CRN environment due to mobility or other reason. Further the conversion of trusted node to malicious during handoff process states that out of 250 handoff 15 nodes are converted to malicious as presented in Table 3. Taking all these assumptions, performance analysis is accomplished for 80 s.

The architecture of proposed framework consists of a TA, responsible for authenticating the legitimacy of CU and HCU, two gateway routers which offer the connectivity among internet & routers and routers which afford the services to CU that essentially employ the internet services.

The TNs are alienated into different zones that provide the services to their zonal or domain's CU as Home Routers (HR). The realms are assembled according to transmission range of CU with their HR

A. System state

Based on test bed formed in Fig. 5 various parameters such as throughput, packet delivery ratio, packet loss ratio, falsification attack, packet delivery ratio, average authentication, maximum authentication and probabilistic scenarios of authentication mechanism have been considered. Initially 25 nodes are assigned to each CRN and after each 80 s, more nodes are assigned in order to test the framework scalability. To assess the recital of proposed framework on the basis of above revealed performance metrics, ns-2 simulator is worn.

B. Existing method

In this paper, the author's have proposed probabilistic scenarios of PUEA false presence [23]. They have proposed a cooperative sensing mechanism with an attack-aware means

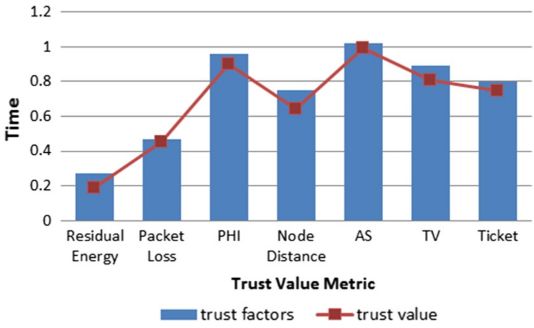


Fig. 6 Relative normalized weights of the TV parameters for handoff routing process

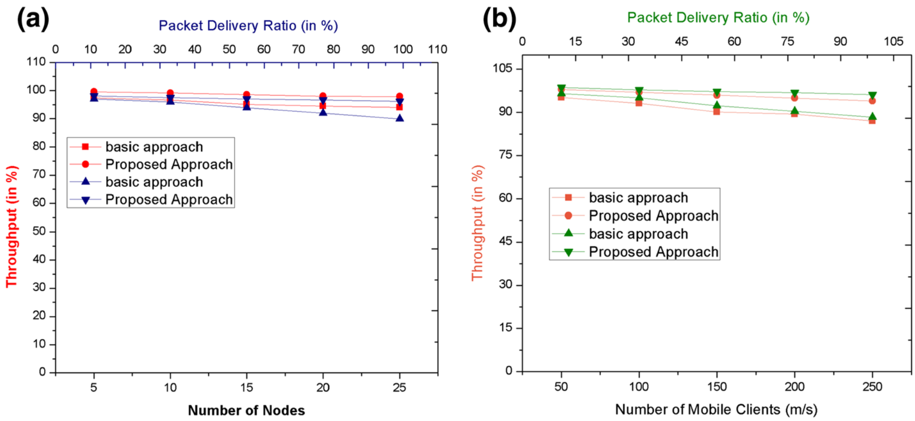


Fig. 7 **a** Network Throughput and Packet Delivery Ratio over small network size. **b** Network Throughput and Packet Delivery Ratio over large network size

during the presence of a false PUEA. The results are obtained with and without the presence of PU. Further, the attained parameter of proposed mechanism performs better and determined a minimized total error probability. As compare to conventional techniques.

C. Performance parameter

Various parameters were recorded for performance comparison of proposed framework against existing approach. In existing mechanism, malicious devices are not detected based on TV. Further increases the computational overhead, key management by increasing the response time of the system. While in case of proposed mechanism, PDL, throughput and authentication process results performs better as they immediately detect and remove the malicious devices/nodes once identified. Figure 6 illustrate relative normalized weights for parameters from depicted Figure it can be clearly seen as PL and authentication server have maximum relative normalized weights in comparison of other parameters and is considered as most significant parameter whereas RE, node distance is considered as least significant parameter. Further Figs. 7, 8 and 9 provides the accuracy of proposed system in comparison of existing approach to detect the MN or CU from the network connected to respective CU's such as throughput, packet delivery ratio, packet loss ratio, end-to-end delay and the possibility of falsification attack. Further, attack resiliency is measured against grey hole

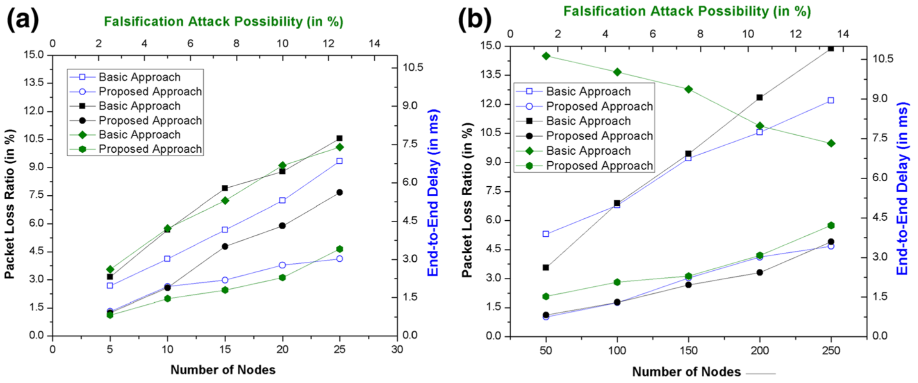


Fig. 8 **a** Packet Loss Ratio and Falsification Attack Possibility over small network size. **b** Packet Loss Ratio and Falsification Attack Possibility over large network size

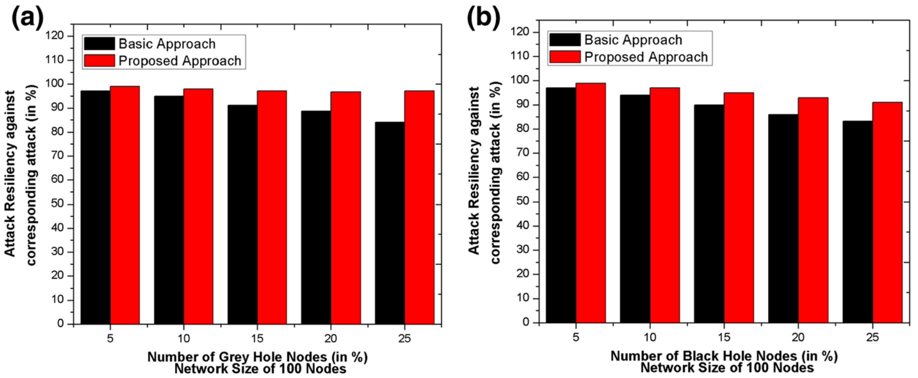


Fig. 9 **a** Attack Resiliency against corresponding attack over a network size of 100 nodes a against worm hole nodes and **b** against black hole nodes

and black hole attacks for smaller and larger network sizes. Figure 10 depicts the CU nodes authentication, probabilistic scenarios based on trust factor and previous history interaction analyzed by AS or TA in both the domains. The proposed framework offers 87% accuracy in comparison of MN and MU prediction that can be further improved if experiment runs for longer period. The measuring parameters in proposed framework perform better in comparison of existing systems.

D. Results discussion

The proposed framework has been assessed based on multiple NN and CUs for which a customized test bed has been proposed. Experiment evaluation accomplished was successful and multiple results regarding various parameters have been recorded. System state and performance parameters results are presented in sub section *A* and *B* respectively. System behaved as preferred and all performance parameters were positive for proposed system for any CRN. Accuracy was close to 87% which will be further improve with time because of removal of detected MNs or MUs from the system. Detection of MNs based on trust

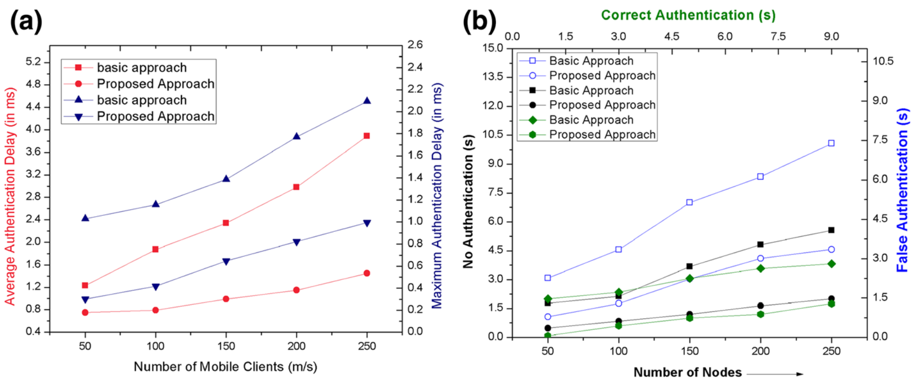


Fig. 10 **a** The effects of number of mobile clients over a) average and maximum authentication. **b** Probabilistic scenarios to measure the authenticity of nodes

and removal of detected MNs or MUs did not hinder the performance of other nodes. The proposed mechanism computes the trust and rating of their nodes after a specific interval of time. The nodes that are compromised and behave maliciously will have low rating and trust (because of high PDR, low throughput etc.) and would never be considered for path formation. Similarly TA computes the TV of the NCU or HCU before allowing the transmission process that further increases the security aspect.

6 Conclusion

This paper has proposed a security framework at certain aspects of communication process in CRNC environment. The handoff communication attacks for both intra-domain and inter-domain processes that are successfully resolved by proposing a TA and ticket based approach. The proposed mechanism efficiently identified the routing attacks in the communication process by computing the TV and have analyzed over network throughput and packet drop ratio over number of MUs and CUs, NCUs and HCUs respectively. Further the proposed mechanism simulation results significantly presented a reduction in network throughput, packet delivery ratio, packet loss ratio, falsification attack, average authentication, maximum authentication and probabilistic scenarios of authentication mechanism respectively. The concept of energy degradation during handoff communication will be considered in further communication.

References

1. Rabbachin, A., Quek, T. Q., Shin, H., & Win, M. Z. (2011). Cognitive network interference. *IEEE Journal on Selected Areas in Communications, 29*(2), 480–493.
2. Mitola, J., & Maguire, G. Q. (1999). Cognitive radio: Making software radio more personal. *IEEE Personal Communication, 6*(4), 13–18.
3. Jabir, A. J., Shamala, S., Zuriati, Z., & Hamid, N. (2018). A comprehensive survey of the current trends and extensions for the proxy mobile IPv6 protocol. *IEEE Systems Journal, 12*(1), 1065–1081.
4. Wang, C. W., & Wang, L. C. (2012). Analysis of reactive spectrum handoff in cognitive radio networks. *IEEE Journal on Selected Areas in Communications, 30*(10), 2016–2028.

5. Gao, R., Ji, X., & Bao, Z. (2018). Secure relay selection of cognitive two-way denoise-and-forward relaying networks. *Wireless Personal Communications, 103*(4), 2957–2976.
6. Sharifiand, A. A., & Niya, J. M. (2016). Securing collaborative spectrum sensing against malicious attackers in cognitive radio networks. *Wireless Personal Communications, 90*(1), 75–91.
7. Rathee, G., Jaglan, N., Saini, H., Gupta, S. D., & Kanaujia, B. K. (2019). "Probabilistic verification scenarios with reduced authentication delay for handoff clients in mesh networks. *Wireless Personal Communications, 104*(1–19), 2018.
8. Val, I., Etxabe, A., Torrego, R., Rodriguez, P. M., Cruces, C., Diez, V., et al. (2019). Design, analysis and implementation of a time-bounded spectrum handoff algorithm for real-time industrial wireless sensor and actuator networks. *Journal of Network and Computer Applications, 125,* 1–16.
9. He, Y., Yu, F. R., Wei, Z., & Leung, V. (2019). Trust management for secure cognitive radio vehicular ad hoc networks. *Ad Hoc Networks, 86,* 154–165.
10. Salwe, S. S., & Naik, K. K. (2018). Wireless network security based on the image address masking (IAM) mechanism. *Wireless Personal Communications, 101*(1), 23–40.
11. Liang, J., Ma, M., Sadiq, M., & Yeung, K. H. (2019). A filter model for intrusion detection system in vehicle ad hoc networks: a hidden Markov methodology. *Knowledge-Based Systems, 163,* 611–623.
12. Rathee, G., Saini, H., & Singh, G. (2018). Aspects of trusted routing communication in smart networks. *Wireless Personal Communications, 98*(2), 2367–2387.
13. Choi, O. K., & Cho, E. (2019). The mechanism of trust affecting collaboration in virtual teams and the moderating roles of the culture of autonomy and task complexity. *Computers in Human Behavior, 91,* 305–315.
14. Dhand, G., & Tyagi, S. (2018). "SMEER: secure multi-tier energy efficient routing protocol for hierarchical wireless sensor networks. *Wireless Personal Communications, 105,* 1–19.
15. Li, X., Niu, J., Bhuiyan, M. Z. A., Wu, F., Karuppiah, M., & Kumari, S. (2018). A robust ECC-based provable secure authentication protocol with privacy preserving for industrial internet of things. *IEEE Transactions on Industrial Informatics, 14*(8), 3599–3609.
16. Chen, H., Zhou, M., Xie, L., Wang, K., & Li, J. (2016). Joint spectrum sensing and resource allocation scheme in cognitive radio networks with spectrum sensing data falsification attack. *IEEE Transactions on Vehicular Technology, 65*(11), 9181–9191.
17. Althunibat, S., Denise, B., & Granelli, F. (2015). Identification and punishment policies for spectrum sensing data falsification attackers using delivery-based assessment. *IEEE Transactions on Vehicular Technology, 65*(9), 7308–7321.
18. Gan, Y., Jiang, C., Beaulieu, N., Wang, J., & Ren, Y. (2016). Secure collaborative spectrum sensing: a peer-prediction method. *IEEE Transactions on Communications, 64*(10), 4283–4294.
19. Vosoughi, A., Cavallaro, J. R., & Marshall, A. (2016). Trust-Aware Consensus-Inspired Distributed Cooperative Spectrum Sensing for Cognitive Radio Ad Hoc Networks. *IEEE Transactions on Cognitive Communications and Networking, 2*(1), 24–37.
20. Liu, Q., Yin, J., Leung, V. C., & Cai, Z. (2013). FADE: forwarding assessment based detection of collaborative grey hole attacks in WMNs. *IEEE Transactions on Wireless Communications, 12*(10), 5124–5137.
21. Li, X., Jia, Z., Zhang, P., Zhang, R., & Wang, H. (2010). Trust-based on-demand multipath routing in mobile ad hoc networks. *IET Information Security, 4*(4), 212–232.
22. Liu, Y., Dong, M., Ota, K., & Liu, A. (2013). Active trust: secure and trustable routing in wireless sensor networks. *IEEE Transactions on Information Forensics and Security, 11*(9), 2013–2027.
23. Sharifi, M., Sharifi, A. A., & Niya, M. J. M. (2018). Cooperative spectrum sensing in the presence of primary user emulation attack in cognitive radio network: multi-level hypotheses test approach. *Wireless Networks, 24*(1), 61–68.
24. Sharef, B., Alsaqour, R., Alawi, M., Abdelhaq, M., & Sundararajan, E. (2018). Robust and trust dynamic mobile gateway selection in heterogeneous VANET-UMTS network. *Vehicular Communications, 12,* 75–87.
25. Din, S., Ahmad, A., Paul, A., & Rho, S. (2018). MGR: multi-parameter green reliable communication for internet of things in 5G network. *Journal of Parallel and Distributed Computing, 118,* 34–45.

Geetanjali Rathee received B.Tech Degree in Computer Science and Engineering from MDU Rohtak, Haryana in the year 2011. She has completed her M.Tech in Computer Science and Engineering from Jaypee University, Waknaghat, Solan in the year 2014. She obtained her Ph.D. in Computer Science and Engineering from Jaypee University, Waknaghat, Solan in the year 2017. Currently, she is working as an Assistant Professor in Computer Science and Engineering Department in Jaypee University, Waknaghat, Solan. Her research interest include resiliency in wireless mesh network, routing protocols, network protocols and security in next generation communication systems, security aspects in cognitive radio network.

Naveen Jaglan was born in 1989, obtained his B.Tech and M.Tech degree in Electronics and Communication Engineering in 2009 and 2011 respectively from Kurukshetra University, Kurukshetra, India. He obtained his Ph.D. degree on Microstrip antennas in Jaypee Institute of Information Technology Noida in 2016. He has authored/co-authored several research papers in referred International Journals and Conferences. He is also a co-author in the Handbook of Research on Advanced Trends in Microwave and Communication Engineering published by IGI Global Publishers USA. His research has included microwave communications, planar and conformal microstrip antennas including array mutual coupling, EBG, PBG, FSS, DGS, novel antennas, UWB antennas, MIMO systems, numerical methods in electromagnetics, composite right/left handed (CRLH) transmissions and High-k dielectrics. His skill includes modelling of antenna and RF circuits with Ansoft HFSS/CST Microwave Studio/ADS Momentum, measurements using Vector Network Analyzer and Anechoic Chamber.

Binod Kumar Kanaujia had completed his B.Tech. in Electronics Engineering from KNIT Sultanpur, India in 1994. He did his M.Tech. and Ph.D. in 1998 and 2004; respectively from Department of Electronics Engineering, Indian Institute of Technology Banaras Hindu University, Varanasi, India. He has been awarded Junior Research Fellowship by UGC Delhi in the year 2001-02 for his outstanding work in electronics field. He has keen research interest in design and modelling of microstrip antenna, dielectric resonator antenna, left handed metamaterial microstrip antenna, shorted microstrip antenna, ultra-wideband antennas, reconfigurable and circular polarized antenna for wireless communication. He has been credited to publish more than 200 research papers with more than 1000 citations with h-index of 17 in peer-reviewed journals and conferences. He had supervised 50 M.Tech. and 20 Ph.D research scholars in the field of microwave engineering. He is a reviewer of several journals of international repute i.e. IET Microwaves, Antennas & Propagation, IEEE Antennas and Wireless Propagation Letters, Wireless Personal Communications, Journal of Electromagnetic Wave and Application, Indian Journal of Radio and Space Physics, IETE Technical Review, International Journal of Electronics, International Journal of Engineering Science, IEEE Transactions on Antennas and Propagation, AEU-International Journal of Electronics and Communication, International Journal of Microwave and Wireless Technologies, etc. Dr. Kanaujia had successfully executed 04 research projects sponsored by several agencies of Government of India i.e. DRDO, DST, AICTE and ISRO. He is also a member of several academic and professional bodies i.e. IEEE, Institution of Engineers (India), Indian Society for Technical Education and The Institute of Electronics and Telecommunication Engineers of India.