User Credibility-Based Trust Model for 5G Wireless Networks

Shivanand V. Manjaragi and S. V. Saboji

Abstract The 5G wireless networks are expected to provide fastest mobile Internet connectivity, efficient network access, capable of handling large amount of data traffic, connecting large number of mobile devices with high-throughput and very-low latency. The new technologies such as cloud computing, network function virtualization (NFV), and software-defined networking (SDN) are being used in 5G wireless networks. The number of small cells in 5G networks creating a heterogeneous network environment (HetNet), where users will join and leave the network frequently causing repeated authenticated vertical handoff across the different cells leading to delay in the network. There are new security requirements and challenges in 5G mobile wireless network due to its advanced features. Therefore, in this paper to deal with secured vertical handoff, a trusted authenticating mechanism is proposed to secularly authenticate the user based on the credibility in 5G wireless networks. It is generating a trust relationship between user, base station, and home networks based on the user credibility and performs quick and secured handoff. The user credibility is comprises the direct credibility and indirect credibility calculation. Based on the user credibility, the trustworthiness of user equipment (UE) is identified and vertical handoff performed without re-authentication across different heterogeneous small cells in 5G wireless networks.

Keywords 5G wireless networks · SDN · Trusted model · User credibility · Secure vertical handoff

S. V. Manjaragi (✉)
Department of Computer Science and Engineering, Hirasugar Institute of Technology, Nidasoshi, Belgaum, India
e-mail: shiva.vm@gmail.com

S. V. Saboji
Department of Computer Science and Engineering, Basaveshwar Engineering College, Bagalkot, India

G. Rajakumar et al. (eds.), *Intelligent Communication Technologies and Virtual Mobile Networks*, Lecture Notes on Data Engineering and Communications Technologies 131,
https://doi.org/10.1007/978-981-19-1844-5_23

1 Introduction

The fifth generation (5G) wireless networks are evolved to provide the wireless connectivity to mobile devices anytime and anywhere and serve the needs of billions of mobile devices and mobile applications [1]. The 5G wireless networks are an evolution of the 4G mobile networks and have more service capabilities. The advanced features of 5G wireless networks are providing 1–10 Gbps connections to end points, 1 ms latency, complete coverage (100%), and high availability (99.99%) [2]. To achieve these requirements, the number of technologies such as heterogeneous networks (HetNet), millimeter wave (mmWave) [3], massive multiple-input multiple-output (MIMO), device-to-device (D2D) communications [4], networking slicing [5], network functions visualization (NFV) [6], and software-defined network (SDN) [7] are adopted in 5G wireless networks. The 5G networks have incorporated software-defined networking (SDN) technology. The SDN separates the networks data forwarding planes and control planes, and the entire network is controlled through a centralized controller [8], which enables flexible network security management and the feature of programmability. The HetNet in 5G can provide 100% network coverage, high capacity, low latency, low cost, low-energy consumption, and high throughput. To support wider network coverage, the different cells such as femtocells, microcells, and relays are deployed in 5G networks, which is creating a heterogeneous environment in 5G network. In 5G HetNet, the user performs frequent vertical handoffs across the different small cells, and therefore, the handover authentication must be efficient and fast to achieve low delay. The major challenges associated with 5G networks include first, the trust establishment among the devices presents in the heterogeneous network to improve the network performance; second, due to ultra-densification of the network devices, the traffic is changing dynamically which is making it difficult to monitor the behavior of the entities in trust calculation; third, to establish the cooperation among the different small cells for the trust calculation, the network entities consume more energy during the information exchange, and also, there is an increase in communication overhead. The architecture of the 5G wireless network with software-defined network is shown in Fig. 1. A handover authentication management module (HAMM) is deployed at the SDN controller of the 5G network, and SDN protocols are installed at 5G base stations (gNBs) and access points (APs) to support SDN-enabled 5G mobile network [9]. The HAMM will track the location of the registered users and prepare the suitable gNB or access points before the user performs vertical handoff with handover authentication process.

The existing security mechanisms include exchange of keys and key agreement schemes whenever user moves across the different network cells. But these schemes have not considered the scenarios where the users have a different credibility values and protect the networks from the risks whenever the users accessing the network services with very low credibility. Traditionally, wireless network security was achieved through cryptographic authentication mechanisms. Cryptographic techniques called as hard security measures [10] providing security solutions through access control, authentication, and confidentiality for messages. A node can be a

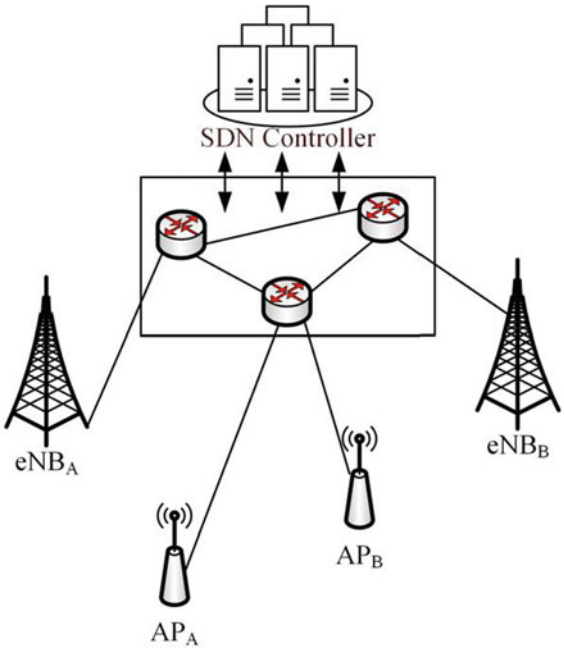

Fig. 1 Architecture of 5G network with SDN

participant in a collaborative group, and it goes through traditional security checkups. However, it may report false measurement results in order to gain access to some service. This type of threat is called soft security threats [10].

Hard security mechanisms have been used to protect system integrity and data may not be protecting nodes from misbehavior by malicious nodes. Through trust and reputation management system, the soft security threats can be effectively eliminated. Recently, the trust-based mechanisms have been used for the security in wireless sensor and ad hoc networks. In wireless sensor networks, the reputations and trust models were used to monitor nodes behavior and used distributed agent-based trust model to identify malicious nodes in the network. The watch dog mechanism was used in sensor networks to collect data, get reputation of each node, and compute trust rating which is broadcasted by the agent node to the sensor nodes. In 5G HetNet, the mutual trust needs to be established between the networks, users, and services with inter-domain user credibility management. There are two types of trust in the networks, namely identity trust and behavior trust. The identity trust can be calculated based on the user authentications, and behavior trust is dynamically calculated based on user behaviors and the previous interactions.

The main contribution of this paper is establishing inter-domain authentication during vertical handoff in 5G HetNet mechanism of roaming network domain will have the access to the trusted service center of the home network domain to obtain the user credibility value, and the user is allowed to access the network entities and services based the credibility value. When the user leaves a network from the roaming

network, the user credibility is updated and sent to the trusted service center of the home network domain. Hence, it is generating a trust relationship between user, base station, and home networks and performs quick and secured handoff across different wireless domains, and its performance is evaluated. The remaining part of this paper is organized as follows. Section II describes the literature review related to trust model in wireless networks. In Section III, the proposed user credibility trust model for 5G wireless networks is described. Lastly, in Section IV, we present the conclusions.

2 Related Work

In last decade, a number of trust models are proposed for heterogeneous wireless networks; in the paper [11], Peng Zhang et al. proposed a dynamic trust model based on credibility of the entity in heterogeneous wireless network to evaluate trustworthiness of networks by considering the factors such as credibility of the target network, credibility of the evaluating entity, direct trust, and recommended trust [11]. But in this model, all the trust values are stored at common entity, and hence, it is non-operative if any fault occurs. In a fuzzy set based trust model for heterogeneous wireless networks [12], the trust is measured by membership degrees of different fuzzy sets and introduced reputation of recommenders and time stamp to evaluate trustworthiness of the candidate network. Israr Ahmad et al. have reviewed the trust management schemes for 5G networks and discussed about applying trust management schemes to improve security in 5G networks including beam forming, channel access, and D2D communication [13]. In [14], the re-authentication delay has been reduced using trust token mechanism and attribute-based encryption cryptography during inter-domain secure handoff over 3G-WLAN integrated multi-domain heterogeneous network. But the total handoff delay is not reduced to meet the requirements of time sensitive applications. A new trusted vertical handoff algorithm in multihop-enabled heterogeneous wireless network [15] is presented which uses multi-attribute decision algorithm to find the nearest relay nodes to access the trust management model, and the performance of the handoff algorithm is increased by 30.7% as compared with the algorithm without considering trust model, but it is increasing computation overhead [15]. The authors in [16] raised a trust-based handoff algorithm by incorporating trust in network vertical handoff management, here the trust similarity model has improved the safety of the algorithm and done relative theoretical analysis. A context aware and multi-service trust model [17] were designed for heterogeneous wireless network, where it assigns dynamic trust score to cooperating nodes according to different contexts and functions in order to determine trustworthiness. The [18] presented a random number-based authentication mechanism with trust relationship between various network elements. In [19], trusted authentication mechanism for vertical handover is presented, where it issues mutually trusted certificates between the entities in the network for the authentication. The watchdog mechanism [20] is used to calculate the credibility of the user based on the node's

current forwarding behavior. The direct credibility and indirect credibility mechanisms are used for credibility degree calculation [21]. The network entities trust model and stakeholder trust models are exist for 5G wireless networks [22], and a trust model with Bayesian network was proposed to determine the trustworthiness of the stake holders. The subjective logic along with cloud computing technology is used to determine the credibility for 5G communication [23]. In the existing trust models, the re-authentication delay is not significantly reduced which is required for 5G network and has not considered the heterogeneous network environment for the trust establishment among the stakeholders. Further, the exchange of trust value with the target network during vertical handoff to avoid the re-authentication is time consuming, and there is additional computational overhead and not considered granting access to the high-security services based on the trust value.

3 Proposed User Credibility-Based Trust Model for 5G Networks

The proposed user credibility trust-based model for 5G wireless network is shown in Fig. 2. The trusted means accessing to specific network and services not only through user identification and authentication but also through the user credibility. Based on the user credibility value, the user is allowed to access the roaming network and

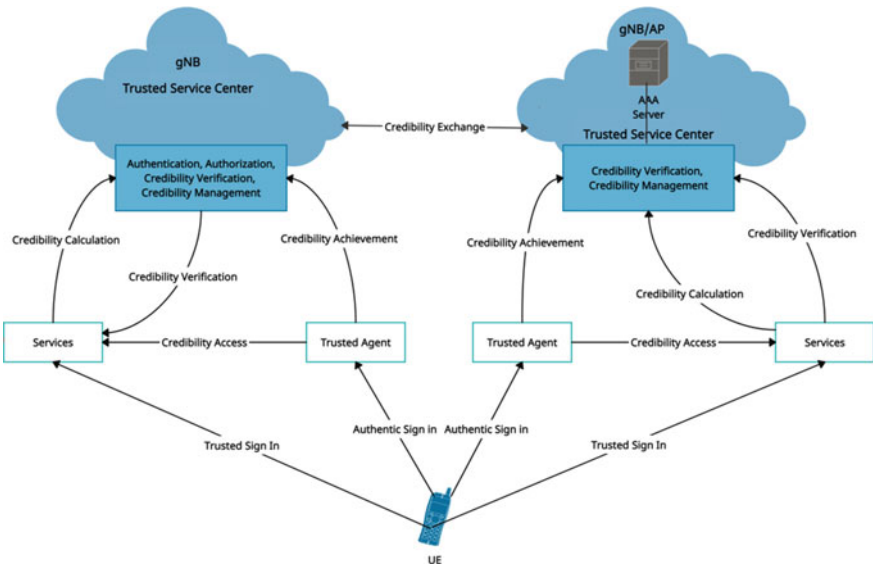

Fig. 2 Trust model for 5G wireless networks

services. During network access period, according to the behavior of the user, their credibility is dynamically updated.

The trusted service center is installed at HAMM of SDN controller in 5G networks as shown in Fig. 2. The trusted service center will manage the credibility of the user and is involved in credibility calculation, credibility verification, and exchange of credibility value with trusted service center of other network or cell in 5G HetNet during vertical handoff. The functionality of the credibility management component is the calculation of the credibility of the user and expressing the credibility in terms of some value. The user is allowed to access the networks and services based on the credibility, and whenever user leaves the network, the credibility parameters such as the number of trusted operations and number of untrusted operations along with time stamp are sent to trusted service center where the credibility of the user is updated based on the their behavior during the network access period. The functionalities of credibility verification component are that when the user request for network access the credibility is verified and the higher credibility value ensures network services access immediately. During vertical handoff, the credibility value of the user which is stored in trusted service center of the home network will be exchanged with trusted service center of the foreign network, and network access is granted based on the credibility of the user. In this model, user will be authorized when user successfully completes the verification of the credibility. The communication trusted agents are responsible for user authentication based on the credibility. If the credibility value of the user is higher than the threshold value, the user will access the services, otherwise the user has to be re-authentication through complete authentication process.

The vertical handoff decision is made based on multiple parameters, namely received signal strength, current load on the target point of access (TPoA), remaining bandwidth that an TPoA can provide, and the credibility of the UE calculated based on direct trust and indirect trust. The TPoA is chosen whenever the received signal strength of the current point of access (CPoA) is less than the desired signal strength, then the vertical handoff is initiated in the heterogeneous wireless network. Next, handoff decision attributes such as received signal strength, current load on the access point, and remaining bandwidth by collecting the target network information. By calculating the credibility value of the all UEs, the untrusted UEs can be prevented from joining the TPoA. In this paper, we are focusing on the user credibility-based trust calculation of the UE before the vertical handoff is performed, which can be used to avoid the re-authentication of the user during handoff and thereby reducing the authentication delay.

The trusted authorization of the UE during vertical handoff is shown in Fig. 3. In the proposed credibility based trust model for 5G HetNet, let us assume that there is a roaming agreement between trusted service center of the current visited network and trusted service center of the home network. Whenever UE is attaching to the current visited access network first time, it will go through full authentication process using packet system authentication and key agreement (EPS-AKA) mechanism by interacting with home network's AAA server, and after successful authentication, UE will be able to use the services of current network. At the time of network access, the credibility of the UE is calculated based on its behavior. Whenever the UE leaves

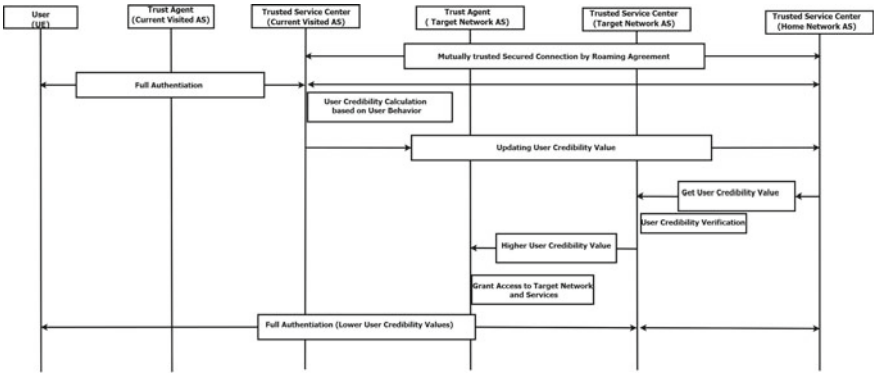

Fig. 3 Interaction diagram showing the credibility calculation and verification

the current access network, the updated credibility value that is accounted during its network access period is forwarded to the trusted service center of the home network and updated. Whenever the UE moves from current network to target network, instead of re-authenticating UE, the credibility value of the UE is fetched from the trusted service center of the home network. During credibility verification phase, if the credibility value is higher than the threshold value, then the network access is granted immediately otherwise UE has to go through full authentication mechanism. We can calculate the credibility value of the UE by monitoring its forwarding behaviors in the periodic time.

3.1 Direct Credibility Degree Calculation

The direct credibility degree is calculated by the history of the direct interactions of UE with access network in a periodic time. Here, we use the packet forwarding behavior of UE, the repetition rate of the packets, and the delay or latency as parameters for direct credibility calculation. The direct trust between UE and AP of the access network is expressed as DC(UE, AP). The direct credibility calculation formula is given as below.

3.1.1 Packet Forwarding Behavior

A malicious node performs attacks such as theft, tampering of information, and injecting error messages. Hence, to detect abnormal behavior of a node directly, we use the packet forwarding behavior parameter. The credibility value from UE to AP for the packet forwarding behavior is given as below:

$$\left.\begin{array}{l} C1_{\text{cur}}^{\text{direct}}(\text{UE, AP}) = 1 - \text{TE} \times (\text{RV} \times S - \text{PV} \times F) \times C_{\text{last}}^{\text{direct}}(\text{UE, AP}), \text{if}(\text{ts} > 0 \,\text{or}\, \text{tf} > 0, C_{\text{last}}^{\text{direct}}(\text{UE, AP}) > 0) \\ C1_{\text{cur}}^{\text{direct}}(\text{UE, AP}) = 1 - \text{TE} \times C_{\text{last}}^{\text{direct}}(\text{UE, AP}), \text{if}(\text{ts} = 0,\ \text{tf} = 0\,, C_{\text{last}}^{\text{direct}}(\text{UE, AP}) > 0) \end{array}\right\} \quad (1)$$

where $C1_{\text{cur}}^{\text{direct}}(\text{UE, AP})$ is the current direct credibility degree, Δt is the interval time between current and last interaction between UE and gNB or access point, and TE is the time element in the direct credibility degree. TE is calculated by $\text{TE} = \Delta t/(\Delta t + 1)$.$C_{\text{cur}}^{\text{direct}}(\text{UE, AP})$ is the direct credibility value of the interactions between UE and AP last time. RV is reward value, and PV is penalty value, where $1 \geq \text{RV} > \text{PVandRV} > \text{PV} \geq 0, \text{RV} + \text{PV} = 1$. RV increases after successful authentication of UE and forwarding behavior, and PV increases after unsuccessful authentication of UE and forwarding has failed. S represents the probability of successful authentication and forwarding of UE, and F represents unsuccessful authentication, failed forwarding of UE at Δt. Here,$S = \text{ts}/(\text{ts} + 1)$, $F = \text{tf}/(\text{tf}+1)$, and ts represents the time of sucessful forewarding, and tf represents the time of the failed forwarding from UE to AP.

3.1.2 Repetition Rate Parameter

The behavior of the node can be determined by the repetition rate of the packets. The repetition of data packets behavior of a node may be reply attack or retransmission of packets due to poor communication link. If the packet transmission rate has slightly increased but less than the threshold value, this behavior may be due to poor communication link. Otherwise, there is a high possibility of replay attack. When the packet repetition rate of a node is higher than the threshold value, the node may be treated as malicious node. The credibility value based on the repetition rate is given in (2).

$$C2(\text{UE, AP}) = \frac{P_{\text{UE,AP}}(t) - \text{RP}_{\text{UE,AP}}(t)}{P_{\text{UE,AP}}(t)} \quad (2)$$

where $P_{\text{UE,AP}}(t)$ is the number of packets sent at time t by UE and $\text{RP}_{\text{UE,AP}}(t)$ is the amount of repeated packets.

3.1.3 Delay Parameter

In the mobile communication, the transmission delay will increase whenever an attacker creates interference in the signal. The transmission delay should be within the range of the tolerance. Whenever UE is forwarding packets to AP, it is treated as a legitimate user if the transmission delay is less than the threshold value of ø. When the transmission delay crosses the threshold value ø, the probability of attack will increase, and the direct trust value is decreased. Due to interference of the signal, there may be transmission delay in the wireless networks communication.

The transmission delay should be lesser than the threshold value. At the time of data packets forwarding by UE to access points, if transmission delay is less than the threshold of ø, we consider UE as the legitimate user. Otherwise, the probability of malicious attacks is increasing, and the direct trust degree is decreased.

$$C3(\text{UE, AP}) = \frac{D_{\text{UE,AP}}(t) - \text{ø}}{\text{ø}} \tag{3}$$

where $D_{\text{UE, AP}}(t)$ is the average transmission delay.

The total average direct credibility value of the user is derived from all above key factors of communication behavior, and it is defined as DC(UE, AP).

$$\text{DC(UE, AP)} = \sum_{k=1}^{N} \frac{C_k}{N} \tag{4}$$

Here, $0 \leq C_k \leq 1$ and hence, the total direct credibility value is $0 \leq \text{DC(UE, AP)} \leq 1$. Sometimes, the malicious node will pretend to be legitimate node to improve its credibility value and perform the attack, and therefore to avoid the false declaration, we also consider the calculating credibility indirectly by third party node.

3.2 Indirect Credibility Degree Calculation

The indirect credibility degree is the direct credibility degree calculated by the access points of the most recently accessed networks. Here, we consider the credibility value of UE provided by most recently used access points which has high similarity with direct credibility value of the currently accessed network. Similarity is the similar level of credibility value of UE calculated by two most recently used access points AP_i and AP_j. The similarity between AP_i and AP_j indicates that they have the nearly same recommendation level of UE as the current access point AP. The formula to calculate the similarity value is given below:

$$S(AP_i, AP_j) = \frac{\sum\left(DC(UE, AP_i) - \bar{C}_{AP_i}\right) \times DC\left(UE, AP_j\right) - \bar{C}_{AP_j}\right)}{\sqrt{\left(DC(UE, AP_i) - C_{AP_i}\right)^2} \times \sqrt{DC\left(UE, AP_j\right) - \bar{C}_{AP_j}\right)^2}} \quad (5)$$

where, $0 \leq S(\mathrm{AP}_i, \mathrm{AP}_j) \leq 1$, $\mathrm{DC(UE, AP}_i)$ is the direct credibility degree of UE with respect to access point AP_i, $\mathrm{DC}(\mathrm{UE}, \mathrm{AP}_j)$ is the direct credibility degree of UE with respect to access point AP_j. Based on the interaction status of UE between AP_i and AP_j, the average credibility degree of UE is $\overline{\mathrm{C}}_{\mathrm{AP}_i}$ and $\overline{\mathrm{C}}_{\mathrm{AP}_j}$, respectively.

By formula (5), the similarity level of AP_i and AP_j can be calculated, and we consider the credibility value of the AP whose similarity is achieved as some threshold $\tau(\tau \geq 0.7)$. Now, the calculation formula of indirect credibility degree IC (UE, AP) is given below:

$$\mathrm{IC(UE, AP)} = \frac{\sum \mathrm{DC(UE, AP)} \times S(\mathrm{AP}_i, \mathrm{AP}_j)}{\sum S(\mathrm{AP}_i, \mathrm{AP}_j)} \quad (6)$$

where $0 \leq \mathrm{DC(UE, AP}_i) \leq 1$. The final credibility value of UE is the summation of direct credibility value and indirect credibility value. The total credibility value of UE is calculated by using formulas (4) and (6). Therefore, we have

$$C(\mathrm{UE, AP}) = \alpha \times \mathrm{DC(UE, AP)} + \beta \times \mathrm{IC(UE, AP)} \quad (7)$$

where $0 \leq C(\mathrm{UE, AP}) \leq 1$, $\alpha + \beta = 1$ and $1 > \alpha > \beta > 0$.

3.3 *Credibility Value Verification*

A UE in 5G heterogeneous wireless network may be represented as < IMSI, ATR > , where IMSI is the identity of an UE and ATR refers to the attributes. In real-time applications, we cannot just depend on attributes because UEs are facing the security attacks. To avoid security attacks, each UE is assigned with a credibility value. Hence, UE in heterogeneous wireless network is represented as < IMSI, ATR, C > , where C is the credibility value of the node, which can be calculated from Eq. (7). The value of C ranges from 0 to 1. The value 0 indicates malicious UE, which is creating security issues, and AAA server cannot maintain trustworthy relation with these type of nodes. The value 1 indicates full trustworthy. The credibility value of a UE can be increased if it has high probability of successful authentications in earlier sessions and packet forwarding. Otherwise, the credibility value of the UE is reduced and eventually that node may be declared as very untrustworthy and unreliable communication.

The trustworthiness of UE can be defined as very untrustworthy, untrustworthy, trustworthy, and very trustworthy based on the credibility value of the UE as given below:

UE_C = Very untrustworthy ($0 \leq C \leq 0.3$).
UE_C = Untrustworthy ($0.3 < C \leq 0.6$).
UE_C = Trustworthy ($0.6 < C \leq 0.9$).
UE_C = Very trustworthy ($0.9 < C \leq 1$).

During vertical handoff across different wireless network domains or cells, whenever the UE moves from current access network to target access network, instead of re-authenticating UE, the credibility value of the UE is fetched from the trusted service center of the home network. During credibility verification phase, if the credibility value of UE is in the range 0.6 and 1, it is considered trustworthy and then network access is granted immediately otherwise UE has to go through full authentication mechanism. For high-security service access from the current network, the credibility value of the UE must be within the range 0.9 and 1.0.

4 Conclusion

The real-time multimedia applications require secured vertical handoff mechanism with minimum authentication delay and signaling cost in the 5G wireless networks to achieve better QoS. In this paper, we proposed a user credibility-based trust model for 5G wireless networks for reducing authentication delay. The inter-domain authentication is established indirectly when the user is roaming. That is the credibility value of the user is calculated based on the earlier successful authentications, the packet forwarding behavior, the repetition rate of the packets, and the delay. Further, the trustworthiness of the user is predicted from direct and indirect credibility calculation mechanism. The user is allowed to access the network, if it is found to be trustworthiness without re-authentication and their by reducing total authentication delay and achieved better QoS.

Acknowledgement This work was supported in part by funding from center of excellence in cyber security (cyseck) of Karnataka State Council for Science and Technology (KSCST) Bangalore, India. Further we acknowledge Dr. S. M. Hatture to be part of this project.

References

1. Sharma S, Panwar N (2016) A survey on 5G: the next generation of mobile communication. Phys Netw Commun 18(2):74–80
2. Understanding 5G: perspectives on future technological advancements in mobile. GSMA intelligence (2014)
3. Qiao J, Shen XS (2015) Enabling device-to-device communications in millimeter-wave 5G cellular networks. IEEE Commun Mag 53(1):208–214

4. Qian Y, Wu G, Wei L, Hu RQ (2016) Energy efficiency and spectrum efficiency of multihop device-to-device communications underlaying cellular networks. IEEE Trans Veh Technol 65(1):367–379
5. 5G security recommendations package #2: network slicing. NGMN Alliance (2016)
6. Zhang J, Xie W, Yang F (2015) An architecture for 5G mobile network based on SDN and NFV. In: Sixth ınternational conference on wireless, mobile and multi-media (ICWMMN2015), pp 86–91
7. Dabbagn M, Hu B, Guizani M, Rayes A (2015) Software-defined networking security: pros and cons. IEEE Commun 53(6):72–78
8. Dabbagh, Hamdaoui (2015) Software defined networking security: pros and cons. IEEE Commun Mag 53(6):75–78
9. Duan X (2015) Authentication handover and privacy protection in 5G networks using SDN. IEEE Commun Mag 53(4):30–35
10. Josang R (2007) A survey of trust and reputation systems for online service provision. Decis Support Syst 43(2):29
11. Zhang P (2009) A dynamic trust model based on entity credibility in heterogeneous wireless network. In: International symposium on ınformation engineering and electronic commerce-2009, 16th to 17th May 2009, pp 66–70
12. Luo X, He X (2010) Fuzzy set based dynamic trust model for heterogeneous wireless networks. In: 2010 second ınternational conference on networks security, wireless communications and trusted computing, pp 249–253
13. Ahmad I, Yau KLA, Lıng MH (2020) Trust and reputation management for securing collaboration in 5G access networks: the road ahead, 8, pp 62542–62560
14. Deng Y, Cao J, Wang G (2015) Trust-based fast ınter-domain secure handoff over heterogeneous wireless networks, pp 205
15. Dan F, Huang C, Zhu J, Wang X, Xu L, Trusted vertical handoff algorithms in mutihop-enabled heterogeneous wireless networks
16. Feng D, Chuanhe H (2013) Mutihop-enabled trusted handoff algorithm in heterogeneous wireless networks. J Netw 8(1)
17. Saied YB, Azzabi R (2013) A context aware and multi-service trust model for Heterogeneous wireless networks, pp 911–918
18. Narmadha R, Malarkkan S (2015) Random number based authentication for heterogeneous networks. In: IEEE ICCSP 2015 conference, pp 1492–1496
19. Prasad, Manoharan (2017) A secure certificate based authentication to reduce overhead for heterogeneous wireless network. In: International conference on advanced computing and communication systems, 06–07 Jan 2017 Coimbatore, Indıa
20. Marti S (2000) Mitigating routing misbehavior in mobile adhoc networks. In: Proceedings of MobiCom. New York
21. Zhang P (2009) A dynamic trust model based on entity credibility in heterogeneous wireless network. In: International symposium on ınformation engineering and electronic commerce, pp 66–70
22. Wong S (2019) The fifth generation (5G) trust model. In: IEEE wireless communications and networking conference (WCNC), 15th to 18th April 2019, pp 1–5
23. Zhiming D (2021) 5G ıntelligent network trust model based on subjective logic. In: IEEE ınternational conference on power electronics, computer applications (ICPECA), 22–24 Jan 2021, pp 541–545
24. Josang A, Ismail R, Boyd C (2007) BA survey of trust and reputation systems for online service provision. Decis Support Syst 43(2):26
25. He X, Zhang P, Huang K (2009) A dynamic trust model based on entity credibility in heterogeneous wireless network. In: International symposium on ınformation engineering and electronic commerce-200), 16th to 17th May 2009, pp 68–70