IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Trust and Reputation Management for Securing Collaboration in 5G Access Networks: The Road Ahead

ISRAR AHMAD[1], KOK-LIM ALVIN YAU[1], (Senior member, IEEE), MEE HONG LING[1], (Member, IEEE), SYE LOONG KEOH[2],

[1]Department of Computing and Information Systems, Sunway University, Selangor 47500, Malaysia
[2]School of Computing Science, Sir Alwyn Williams Building, University of Glasgow, Glasgow G12 8RZ, Scotland, UK

Corresponding author: Kok-Lim Alvin Yau (e-mail: koklimy@sunway.edu.my).

This work was part of the project entitled "A Novel Clustering Algorithm based on Reinforcement Learning for the Optimization of Global and Local Network Performances in Mobile Networks" funded by the Malaysian Ministry of Education under Fundamental Research Grant Scheme FRGS/1/2019/ICT03/SYUC/01/11.

ABSTRACT Trust represents the belief or perception of an entity, such as a mobile device or a node, in the extent to which future actions and reactions are appropriate in a collaborative relationship. Reputation represents the network-wide belief or perception of the trustworthiness of an entity. Each entity computes and assigns a trust or reputation value, which increases and decreases with the appropriateness of actions and reactions, to another entity in order to ensure a healthy collaborative relationship. Trust and reputation management (TRM) has been investigated to improve the security of traditional networks, particularly the access networks. In 5G, the access networks are multi-hop networks formed by entities which may not be trustable, and so such networks are prone to attacks, such as Sybil and crude attacks. TRM addresses such attacks to enhance the overall network performance, including reliability, scalability, and stability. Nevertheless, the investigation of TRM in 5G, which is the next-generation wireless networks, is still at its infancy. TRM must cater for the characteristics of 5G. Firstly, *ultra-densification* due to the exponential growth of mobile users and data traffic. Secondly, *high heterogeneity* due to the different characteristics of mobile users, such as different transmission characteristics (e.g., different transmission power) and different user equipment (e.g., laptops and smartphones). Thirdly, *high variability* due to the dynamicity of the entities' behaviors and operating environment. TRM must also cater for the core features of 5G (e.g., millimeter wave transmission, and device-to-device communication) and the core technologies of 5G (e.g., massive MIMO and beamforming, and network virtualization). In this paper, a review of TRM schemes in 5G and traditional networks, which can be leveraged to 5G, is presented. We also provide an insight on some of the important open issues and vulnerabilities in 5G networks that can be resolved using a TRM framework.

INDEX TERMS Next-generation networks, 5G, Cooperation, Trust and reputation management, Artificial intelligence

I. INTRODUCTION

5G is the next-generation wireless network that aims to improve spectral efficiency and energy efficiency in the presence of a large number of mobile devices (or nodes) and data traffic in order to increase data rate (or network capacity), as well as to reduce latency and energy consumption [1], [41]. Figure 1 shows a 5G network that must cater for the next-generation network characteristics, including: a) *ultra-densification* in which there is a significant increase in the number of network entities (e.g., the number of small cells, such as pico cells and femto cells, in an area); b) *high heterogeneity* in which there are different network entities (e.g., network cells and devices), network characteristics or scenarios (e.g., indoor and outdoor), user requirements (e.g., quality of service), and so on; and c) *high variability* in which bursty traffic (or network traffic that changes significantly) causes insufficiency and surplus of bandwidth within a short period of time. Network entities, such as network cells and user devices, must cooperate and coordinate with each other via message exchange to perform cooperative tasks in order

to enhance the overall network performance (e.g., end-to-end delay, successful packet transmission rate, and scalability). Examples of cooperative tasks are: a) *cooperative communication* that enables neighboring nodes to cooperate with each other and work as relays to forward information or packets to intended destinations [42]; b) *channel access* that enables neighboring entities to gather network information about channel availability; and c) *clustering* that enables nodes to segregate themselves into logical groups in order to enhance network stability and scalability. While cooperation is important for network functionalities [22], [52], it has opened door to various security vulnerabilities, particularly in access networks. A successful cooperation must remove or reduce the detrimental impacts of malicious or misbehaving entities as time goes by. Trust and Reputation Management (TRM), which is embedded in an entity, calculates the trust and reputation values of another entity in an independent manner [21], or in cooperation with neighboring entities [4], [5], or a third party entity [50]. TRM rewards and increases the trust or reputation values of legitimate entities, as well as punishes and reduces the trust or reputation values of malicious or misbehaving entities, as time goes by. This helps to identify malicious or misbehaving nodes so that countermeasures, such as to remove them from collaboration and to reduce their detrimental impacts to cooperation, can be taken. The unique characteristics of next-generation networks, including ultra-densification, high heterogeneous, and high variability, have brought about new challenges to the provision of TRM in 5G.

Traditional security measures, such as cryptography [2], [12], and intrusion detection systems [12], [40], which provide confidentiality, integrity and authentication, provide security services to countermeasure external attacks (e.g., man-in-the-middle [2] and eavesdropping [2], [40]) at the application layer. In contrast, TRM provides security services to countermeasure both external and internal attacks, such as crude [33], [35], [53], wormhole [21], [50], [53], black hole [4], [5], [35], and routing loop [5], [34], [50], attacks at lower layers, particularly the network and data link layers (see Table 5, for more details). For instance, TRM continuously monitors the trust and reputation values of nodes despite a successful initial authentication so that any changes of behaviors from legitimate to malicious can be detected.

A. CONTRIBUTIONS

This paper presents a review of the state of the art of TRM in 5G, as well as other networks, particularly cognitive radio networks (CRNs), vehicular ad-hoc networks, and 4G, which can be leveraged to 5G. This paper focuses on TRM in access networks, rather than core networks. The review is necessary as collaboration is essential to various schemes in 5G access networks, including channel access, channel sensing, interference mitigation, and collaborative applications that require content sharing, and TRM has shown to detect malicious nodes and manipulated data efficiently in collaboration. Various aspects of TRM are covered, including objectives, challenges, characteristics, attacks, and performance metrics; and these aspects are related to the state of the art. This paper also explains various open issues that can be explored to further enhance TRM in 5G.

B. ORGANIZATION OF THE PAPER

The rest of this paper is organized as follows. Section II presents background and the roles of TRM in 5G. Section III focuses on the taxonomy of TRM in 5G. Section IV presents a TRM framework covering the mechanisms of TRM. Section V presents existing TRM schemes in 5G. Section VI presents open issues, and finally Section VII concludes the paper.

II. BACKGROUND AND THE ROLES OF TRM IN 5G

This section presents the background of 5G, including its architecture and new features with emphasis on the security vulnerabilities of the new features that are brought about by their needs for collaboration in 5G. This section also presents the background of TRM with the main interest on the roles of TRM in addressing the security vulnerabilities of the new features of 5G. Further description about TRM in 5G, including its challenges, is presented in Section III.

A. WHAT IS 5G?

5G is the next-generation wireless network aspired to achieve high data rate (or network capacity), as well as low latency and energy consumption. Table 1 summarizes some notable differences and significant improvement in terms of network performance in 5G as compared to 4G.

1) 5G Architecture

5G uses a control-data separation architecture (CDSA) in which the control and data planes are available in separate hardware devices in 5G. However, they are tightly coupled in a single hardware device in traditional networks. The control plane, which has controllers and network-wide information, performs management and services, such as routing and resource allocation, that impose policy on the data plane; while the data plane performs data storage and forwarding [1]. Specifically, the functions of the control plane are performed using software running based on software-defined networking (SDN) [14], [40], network function virtualization [34], [40], and network slicing [14], and the functions of the data plane are performed using less complex user devices in 5G. Hence, 5G provides programmability and reconfiguration. On the other hand, both control and data planes are performed by specialized hardware devices, such as routers and switches, in 4G.

Figure 2 shows that: a) macro cell, which serves as the control plane, has the largest coverage at the expense of lower data rate because lower frequency bands (e.g., less than 2 GHz) are used; and b) small cell (i.e., pico and femto cells), which serves as the data plane, has smaller coverage although it has higher data rate because higher frequency

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2984318, IEEE Access

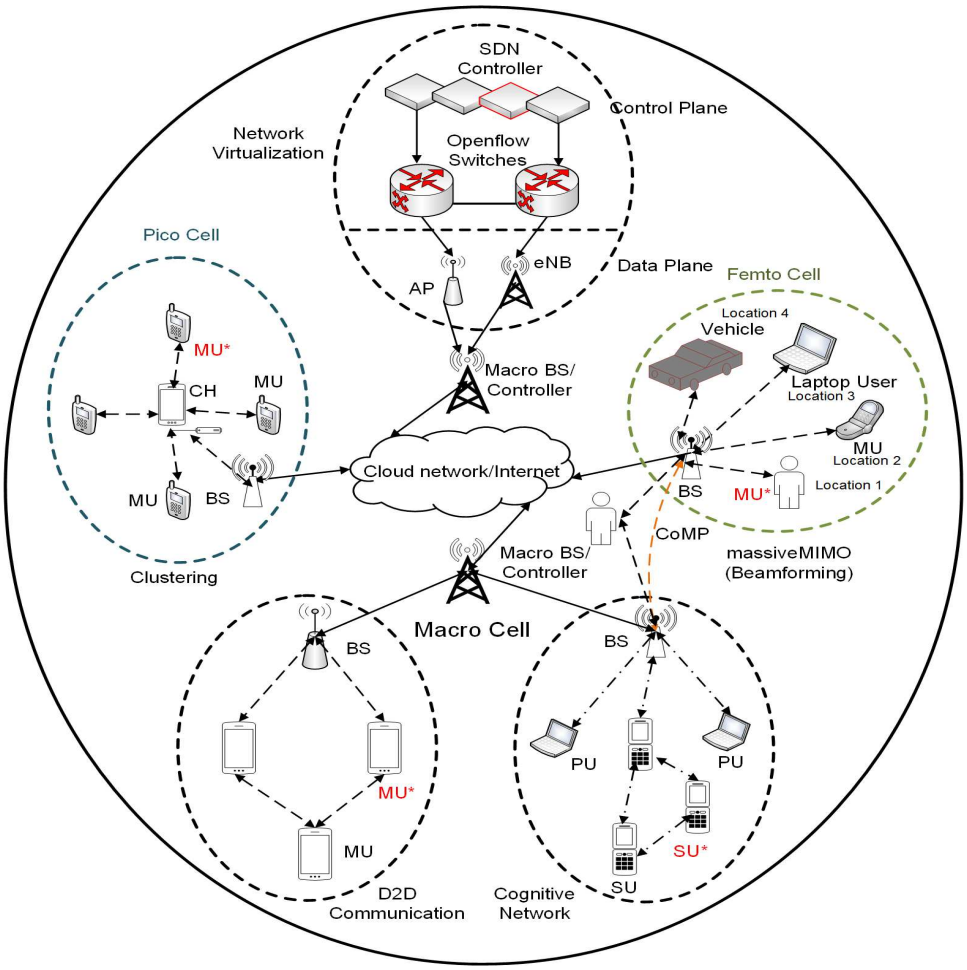


FIGURE 1: The features and cooperative scenarios of 5G wireless networks. These include SDN, clustering, D2D communication, beamforming, CoMP, and CRN. The malicious users MU* are characterized by high heterogeneity and ultra-densification in the presence of various kinds of network cells and user equipment (UE) such as mobile (MU), laptop, cluster head (CH) as relay node, including macro cell, small cells (i.e., pico and femto cells), base stations (BSs)/controllers, and cloud.

TABLE 1: Comparison between 4G and 5G

Category	Details	Performance enhancement	
		4G	5G
Performance	Data rate	Up to 1 Gbps	Up to 20 Gbps
	Spectral efficiency	30 bps/Hz	120 bps/Hz
	Latency	10 ms	1 ms
	Mobility support	Up to 350 Km/h	Up to 500 Km/h
	Energy efficiency	0.1 mJ/100 bits	0.1 μJ/100 bits
Channel	Frequency band	2–8 GHz	2–300 GHz
	Connection density	1,000/km^2	1,000,000/km^2

bands (e.g., mmWave or more than 30 GHz) are used. TRM has been investigated to improve the security of UE in access network, whereby UEs form a multi-hop network and may connect to BSs [6], [17], [39]. However, TRM has not been investigated to improve the security of BSs in the network core, whereby multiple BSs from different network cells communicate with each other [16], [54]. Both macro cell and small cells can use different frequency bands. As an example, high transmission power and low frequency bands are used to provide long-range transmission (as shown using solid lines in Figure 2). As another example, low transmission power and high frequency bands are used to provide short-range transmission (as shown using dotted lines in Figure 2). The base station (BS) of each network cell has different kinds of radio access technologies (RATs) to access licensed (or cellular) and unlicensed (or cognitive) channels; contributing to the heterogeneous nature of 5G. In addition, the BS of the macro cell is connected to the cloud, which provides access to a central controller. The central controller collects network-wide information on traffic characteristics (e.g., traffic pattern, congestion level, and interference level), network performance, network resources (e.g., computing and storage capabilities), and network services (e.g., medium access control, route selection, and resource allocation).

Cognition (or intelligence) can be incorporated in macro cells, small cells, and the central controller to make intelligent decisions. Artificial intelligence approaches, such as reinforcement learning (RL) [34], and its deep variant called deep reinforcement learning (DRL) [25], [58], enable an agent (or decision maker such as the central controller and BS) to observe and learn from the operating environment. In order to use the artificial intelligence approach, the three main representations of RL and DRL, namely *state*, *action*, and *reward*, must be designed. The state represents the decision making factors (e.g., the estimates of trust values) that affect action selection and reward. The action represents a selected action, such as a forwarding entity (or node). The reward represents network performance (e.g., packet delivery rate, malicious node detection rate, and false alarm) achieved by the agent for taking the action under the state, which may either improve or deteriorate. As an example, artificial intelligence can be used by network cell BSs to choose the right RAT so that they can establish communication with their nodes with higher quality of service (QoS) and quality of experience (QoE). The agent is embedded in each network cell BS. The state represents radio frequency (i.e., lower or higher frequencies), the action represents the selection of an ideal radio technology to communicate, and the reward represents successful packet delivery rate, which is a QoS performance metric. As another example, artificial intelligence can be used by network cell BSs to adjust their transmission power so that they can reduce inter-cell interference with both neighboring and overlapping network cells, which helps to improve channel sharing. Similarly, the agent is embedded in each network cell BS. The state represents the coverage or position of a user or network entity, the action represents a beam towards the user or network entity, and the reward represents the reduced interference level.

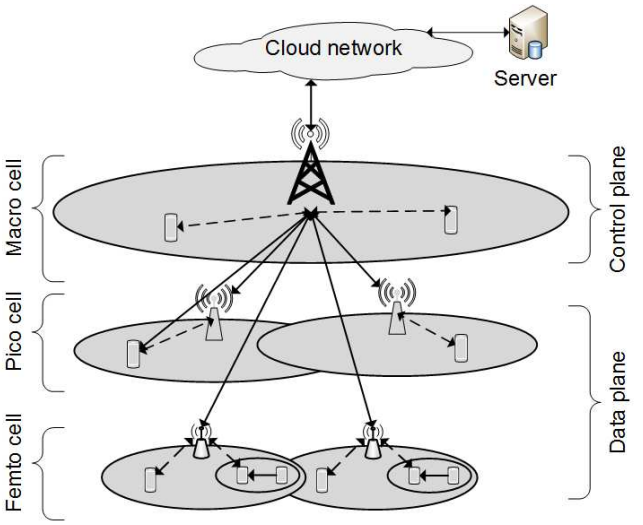


FIGURE 2: 5G architecture. Macro cell, pico cell, and femto cell overlap among themselves. Macro cell handles the control plane and is connected to the cloud network, which consists of the central controller or management node, via backhaul. Dotted lines represent communication in a network cell, such as data transmission from one UE (or network device) to another UE via a relay UE (or service node). Solid lines represent communication between network cells, such as control message exchange between macro cell and small cell BSs (or terminals). For simplicity, BS refers to terminal, UE refers to network device, relay UE refers to service node, and central controller refers to management node.

Table 2 summarizes the characteristics of macro cell, pico cell, and femto cell. The macro cell has the largest coverage, the highest transmission power, and the highest number of users supported. The largest coverage is attributed to the use of lower frequency bands that provide higher penetration power and longer propagation distance. The small cells (i.e., pico cell and femto cell) have smaller coverage, lower transmission power, and lower number of users supported. The small cells are suitable for small areas. For instance, pico cell can be used in the university and airport compounds, and femto cell can be used in the indoor environment. Nevertheless, the small cells provide: a) higher data rate because higher frequency bands (e.g., mmWave or 2-300 GHz frequency bands) and beamforming with multiple MIMO for directional transmission are used; b) lower delay because of local processing at close proximaty BSs; c) lower energy consumption because of communication among close proximity BSs and nodes; and d) higher connectivity and larger coverage because of its coverage extension. Small cells can offload traffic from the macro cells.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2984318, IEEE Access

TABLE 2: Characteristics of network cells

Cells	Coverage	Transmission power	Users
Macro	1-30 km	5-25 watts	Upto 1000
Pico	100-250 m	250 mw	32-64
Femto	10-50 m	100 mw	8-16

2) 5G Features

Collaboration requires different network entities to share information and make intelligent decisions based on collective information in order to improve network performance. However, malicious entities can exploit collaboration to reduce network performance. One common method is that the malicious entities manipulate the information being exchanged among the network entities in order to affect the final decision. TRM assists network entities to calculate trust or reputation values, identify, and isolate malicious entities from collaboration. The security vulnerabilities of the collaboration required in various new features being introduced in 5G, as shown in Figure 1, can be exploited as shown below.

- *Massive multiple-input and multiple-output (MIMO)* uses an array of antennas (e.g., 16 antennas per sector [24]) at transceivers so that multiple mobile users can communicate with a BS simultaneously, leading to a higher beamforming gain, as well as spectral and energy efficiencies. Nevertheless, the use of a large number of antennas can increase interference, computational complexity, and hardware cost. Cooperation enables network entities (e.g., BS) equipped with antennas at different locations to direct transmission in different locations in order to reduce interference using beamforming. However, when malicious or misbehaving network entities share and exchange manipulated information (e.g., location information), direct transmission in the inaccurate or wrong direction can cause interference.

- *Millimeter wave (or mmWave) transmission* allows nodes to communicate in the frequency bands between 3 GHz to 300 GHz, providing a high data rate of up to 20 Gbps, which improves spectal and energy efficiencies. This means that the operating frequency bands from 2 to 8 GHz in the conventional 4G networks must be extended to higher frequency bands (i.e., 8-300 GHz) [10], [36]. Nevertheless, mmWave has a high frequency range and so it has short wavelength, resulting in poor penetration through obstacles and high propagation loss [36]. In other words, mmWave is suitable for short-range communication. Collaboration enables network entities to share channel availability information (e.g., channel sensing outcomes) so that transmission can be made in the right channel. However, malicious and misbehaving network entities can cause interference. The malicious nodes share and exchange manipulated channel availability information, and so the legitimate network entities may not access available channels causing reduced bandwidth availability, and may access unavailable channels causing interference.

- *Device-to-device (or D2D) communication* allows neighboring nodes to communicate with each other directly without going through the BS in order to increase data rate, as well as reduce latency and energy consumption. Collaboration enables network entities to share information so that the proximal nodes, which are located within a particular distance with each other, can benefit from each other in a diverse range of applications (e.g., content sharing and public safety) via collaboration and communication. However, when malicious nodes share manipulated information with other nodes, the inaccurate information or malicious codes can affect other nodes' trust value and deteriorate network performance.

- *Dynamic channel access* allows nodes to sense for and use white spaces (or underutilized channels), which can be in the conventional or mmWave frequency bands, in order to improve spectral efficiency. Similar to cognitive radio, distributed or cooperative channel sensing enables unlicensed or secondary users (SUs) to sense for underutilized channels and share sensing outcomes amongst themselves in order to make final decisions on channel access, which is more accurate as compared to channel sensing performed by individual SUs [7], [13], [31], [45]. The characteristics of 5G networks, including ultra-densified, highly heterogeneous, and highly variable, have posed new challenges to collaboration. For instance, the highly variable data traffic that changes abruptly and unexpectedly increase the difficulty to detect malicious and misbehaving SUs. Cognition or artificial intelligence has been the enabler for nodes to make intelligent decisions. Collaboration enables SUs to share channel availability information (e.g., channel sensing outcomes) so that SUs can make the right decision on channel availability. However, when malicious and misbehaving SUs share and exchange manipulated channel availability information, they cause higher interference (i.e., unavailable channels are reported to be vacant and consist of white spaces) and lower bandwidth availability or channel utilization (i.e., available channels are reported to be occupied) to legitimate SUs [13], [37], [45]. While existing works [13], [37], [45], show that TRM is feasible and can be used to tackle such security vulnerabilities, securing the exploration and exploitation of white spaces, which is a new 5G feature that does not exist in 4G, is yet to be solved. TRM is still at its infancy in 5G and it must cater for the 5G characteristics.

- *Clustering* segregates nodes into clusters or logical groups in order to increase network scalability, reduce control overhead and energy consumption, as well as to support collaboration [47]. Each cluster consists of a cluster head (CH) and cluster members (CMs). The

CH is the leader of a cluster and CMs are the member of the cluster. Clustering addresses heterogeneity, whereby nodes with the same characteristics form clusters and share information via D2D [28]. In the multi-hop scenario, CMs can send data through CH that forward packets towards the destination. There are two main mechanisms in clustering, namely cluster formation and cluster maintenance. *Cluster formation* selects CH and CMs using metrics such as the residual energy level and mobility of neighboring nodes, channel availability, and so on. In this collaboration, channel sensing outcomes can be sent from CMs to CH; subsequently, the CH makes final decision on channel availability for channel access. *Cluster maintenance* allows nodes to re-elect CHs, as well as join and leave clusters as time goes by. However, when the malicious nodes share and exchange manipulated clustering metrics and information, malicious nodes: a) can be selected as clusterheads; and b) can join a cluster. Subsequently, the malicious nodes share and exchange manipulated information in a cluster, affecting essential tasks that require collaboration such as data aggregation [38].

- *Network virtualization* decouples control and data planes in order to provide virtually centralized environment for processing and managing heterogeneous networks, devices, and resources. A controller, as the main component of network virtualization, is used to make policies for the control and data planes according to the users/ applications requirements. The controller is flexible and programmable, where interfaces can be modified according to the user/ application requirements. For instance, mobile network operators can allocate network resources to fulfill the user/ application low latency requirement by providing radio access to the network edge [49]. Cooperation enables multiple controllers to share information and make globally optimized and consistent decisions in multi-controller environment. However, malicious or misbehaving: a) controllers can share and exchange manipulated information (e.g., inaccurate policies for resource allocation); and b) applications can provide manipulated information and codes via the open programmable interfaces. Consequently, both vertical (i.e., the controller itself in the control plane) and horizontal (i.e., the other controllers and network entities in the data plane) components can be affected, causing inappropriate policy or decisions made for routing or resource allocation [34], [40], [49].
- *Coordinated multipoint (or CoMP)* enables network entities to share channel state information, which is used to make intelligent decisions on the selection of BSs to serve nodes in order to reduce inter-cell interference [11], and improve spectral efficiency under ultra-densified and heterogeneous environment. CoMP is essential to reduce the high inter-cell interference caused by the deployment of a large number of small cells that communicate using low transmission power and high frequency bands (i.e., the mmWave frequency bands). The small cells provide short-range transmission that provides higher data rate, as well as lower latency and energy consumption, to cater for ultra-densification. When malicious or misbehaving BSs share manipulated information (e.g., bandwidth requirement) about UEs with other BSs, and nodes associate with the BSs, inter-cell interference and network performance can be affected [8].

B. WHAT IS TRM?

The main difference between trust and reputation is that, while trust is the belief of an individual entity in another entity [23], reputation is the collective belief (or aggregated opinion or global perception) of a group of entities in another entity in a network community [32]. Nevertheless, both trust and reputation depend on a node's historical actions, and they are directly proportional to each other; specifically, an entity with a higher reputation value has a higher trust value, and vice-versa.

TRM detects and removes malicious and misbehaving entities that manipulate information from collaboration [41], [52], in order to improve data authenticity and to minimize the detrimental effects, including false positives (i.e., the false detection rate of legitimate entities instead of the malicious entities). TRM is necessary because mistrust can arise when some entities behave maliciously in an intentional or unintentional manner to gain self-benefit (e.g., increasing the trust values of the entities in order to promote themselves as trusted entities) or to disrupt services. The reputation value can be shared among entities in a collaboration.

C. WHAT ARE THE ROLES OF TRM IN 5G?

This section presents how TRM can solve and mitigate security vulnerabilities in collaboration, which is essential to 5G (see Section II-A2). In general, there are *three* types of malicious and misbehaving characters.

- *Faulty* in which entities have hardware or software malfunctions.
- *Selfish* in which entities gain benefits at the expense of other entities.
- *Malicious* in which entities influence other entities or network operations/ activities negatively.

Cooperation among heterogeneous entities is anticipated in 5G. At the network level, there are different kinds of network cells, particularly macro cells and small cells (i.e., pico cells, and femto cells), to improve network capacity and coverage in order to address ultra-densification. At the device level, there are different kinds of network entities that cooperate to perform essential functions in 5G, such as dynamic channel access, clustering, CoMP, and D2D, that require information sharing and exchange. The network entities can behave ma-

liciously (e.g., sharing manipulated information) and affect decisions made on collaboration in order to reduce network performance. For instance, the malicious and misbehaving entities can launch attacks, such as Sybil (A.1) and denial of service attacks (A.3) against D2D. Due to the extensive reliance on D2D, many essential functions such as traffic offloading, packet forwarding, and information sharing, are affected, resulting in reduced network performance (e.g., higher energy consumption and latency). TRM assists network entities to calculate trust and reputation values in order to identify and isolate malicious nodes from cooperation, which is essential for information sharing and aggregation.

D. WHICH PART OF THE 5G NETWORK USES TRM IN LOWER LAYERS?

TRM has been investigated to improve the security of both application (or upper) and lower layers in 5G. In general, the application layer uses traditional security measures, such as cryptography and intrusion detection systems, to countermeasure external attacks and ensure trusted systems. On the other hand, the lower layers must calculate the trust and reputation values to identify and isolate malicious nodes. While TRM has been investigated in access networks, it has not been well investigated in core networks. This is because core networks are traditionally closed trusted networks established by national or multinational corporations on the basis of trust among network operators [44]. Since the core networks are accessed by a few trusted network operators only, security measures are not incorporated in some core networks (e.g., SS7 core networks [44]). Moreover, core networks can reject packets from malicious entities in the access networks [51]. On the other hand, the access networks, whereby UEs, which may not be trustable, form a multi-hop network, and so such networks are easier targets for attack and prone to trust and security challenges [51]. 5G access network is distinguished from the existing cellular networks which are centralized in nature, and is distinguished from the traditional multi-hop networks due to its complexity characterized by ultra-densification, high heterogeneity, and high variability. The need to secure 5G access networks becomes essential for the essential distributed schemes, such as channel access, channel sensing, interference mitigation, content sharing, and so on.

However, the belief of core networks being closed trusted networks is no longer safe with the convergence and incorporation of new technologies, as well as deregulation, and some works, particularly the application layer solutions, have emerged recently [44]. While our focus is the access network, we have provided some open issues related to the core networks, particularly addressing security vulnerabilities in network virtualization in Section VI-A.

E. WHAT ARE THE COMMON TECHNIQUES TO IMPLEMENT TRM IN 5G?

This section presents different techniques that can be used and leveraged to implement TRM in 5G networks. There are *four* main techniques as follows:

- TRM approaches based on rules calculate trust values based on various metrics, such as the energy level [5], and compared the trust values with thresholds. In [21], the reputation and trust values of entities are used to adjust the contribution of the information received from them.
- Probabilistic TRM approaches, such as the Dempster-Shafer theory [25], calculate probabilities used to synthesize trust values of entities. The probabilities are calculated based on various metrics, such as packet forwarding rate, delay, integrity, and so on. In [53], entropy is used to minimize the subjectivity of monitored metrics and maximize the accuracy of the decisions made on identifying malicious entities.
- Artificial intelligence-based TRM learns about states (e.g., trust value, channel condition, and computation capability) from the operating environment or neighboring entities, takes actions (e.g., the selection of a collaborative entity in collaboration), and receives rewards (e.g., revenue and performance enhancement) from the operating environment [20].
- Blockchain-based TRM allows network entities to use blocks to exchange and collect trust values about a subject entity from neighboring network entities, and calculate the trust value of the subject entity in a distributed manner. Subsequently, network entities with credible information incorporate the trust value of the subject entity into the block of the blockchain [50].

Further description about the TRM approaches is presented in Section V.

III. TAXONOMY OF TRUST AND REPUTATION IN 5G WIRELESS NETWORKS

This section presents and explains the taxonomy of TRM in 5G as shown in Figure 3.

A. TRM OBJECTIVES

Collaborating entities establish trust to share information and make reliable relationship. There are *three* main objectives of TRM in 5G.

O.1 *Trust establishment:* Network entities, such as nodes and BSs, may be heterogeneous and are connected to licensed or unlicensed RATs, and they may collaborate to improve network performance. To establish trust in collaboration, they share direct or indirect information for trust computation. However, malicious or selfish nodes may manipulate the information prior to the dissemina-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2984318, IEEE Access

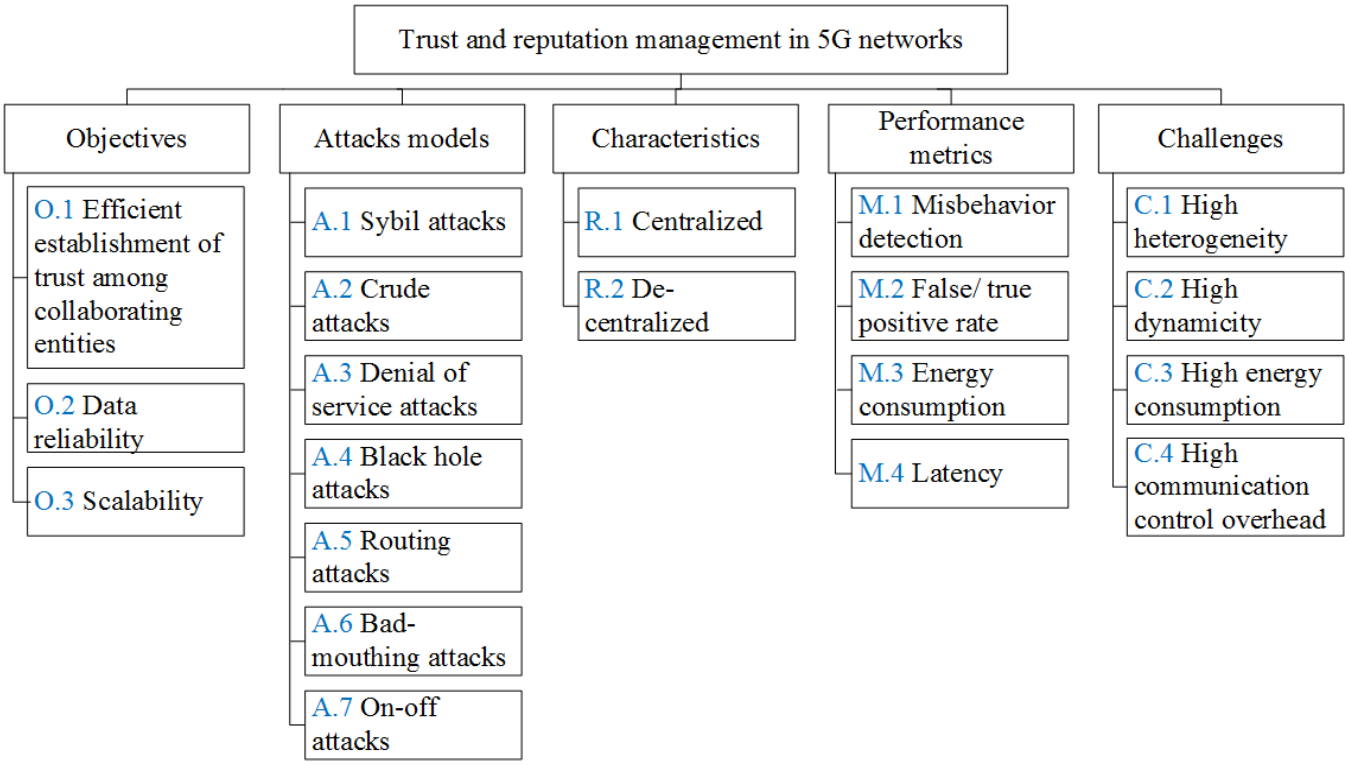


FIGURE 3: Taxonomy of trust and reputation in 5G.

tion of information leading to various kinds of attacks, such as bad-mouthing (or ballot-stuffing) attacks [50], and black hole attacks [4], [53]. For instance, malicious nodes that launch bad-mouthing attacks provide false recommendations of itself or other nodes in order to raise its own trustworthiness and reduce other nodes' trustworthiness. TRM detects and removes malicious network entities from collaboration in order to establish trust among network entities. This means that, while malicious network entities may exist in a network, they are functionally removed from the network.

O.2 *Data reliability:* Network entities share direct and indirect information (e.g., opinion about other nodes) in a collaborative environment to make the decision impactful. The malicious or the selfish network entities alter the information and propagate it for their advantage or with malicious intention (e.g., increasing interference with licensed or primary users or among network cells), resulting in the degradation of network performance. TRM detects and removes malicious network entities from collaboration in order to increase the number of legitimate network entities, and hence improves data reliability (e.g., the accuracy of channel sensing outcomes).

O.3 *Scalability:* Network entities despite being highly heterogeneous (e.g., possess different RATs and network cells) and variable (e.g., traffic and requirements dynamics), collaborate among themselves to make intelligent decisions while providing services and managing resources to be more scalable in terms of the number of supported users. For instance, the right RATs are selected to fulfill the QoS and QoE requirements. Malicious nodes may provide false information about channel access to increase interference among network cells, whereby the scalability of the network is affected. TRM detects and removes malicious nodes from collaboration to improve scalability.

B. CHARACTERISTICS

There are *two* main characteristics for TRM.

R.1 *Centralized:* In a centralized TRM model, a central entity, such as a macro cell BS, a fusion center (FC), or a centralized server, collects and stores data, as well as calculates, monitors, and distributes the globally computed trust value of each network entity among the network entities in the network, as shown in Figure 4a. Specifically, the central entity rewards and punishes network entities based on their behaviors by rewarding legitimate network entities with higher trust values, and punishing malicious network entities with lower trust values. In [21], [30], [50], the central entity is assumed to be trusted, and it provides data collection, calculation, storage, and trust dissemination services; however, due to the highly heterogeneous and dynamic 5G network, it affects QoS (e.g., delay and spectrum

efficiency). In [30], the vehicles sense an event regarding the traffic, and broadcast messages to other vehicles. The credibility of the vehicles are checked and given some feedback, which is then forwarded to the central entity. The central entity calculates decision based on the feedback, updates the trust value, and releases certificates to vehicles in the network. Nevertheless, there are two main shortcomings: a) the centralized TRM model must cater for the massive amount of heterogeneous and highly variable data and network entities in the next-generation networks; and b) it is prone to single point of failure that can affect the availablity of TRM, resources, and services.

R.2 *Decentralized:* In a distributed TRM model, distributed entities, such as small cell BS, UE, or an edge server in edge computing [21], collect and store data, as well as calculate, monitor, and distribute locally computed trust values of network entities among themselves in the network, as shown in Figure 4b. Specifically, a UE calculates the trust value of a neighboring UE either through direct interaction with the UE, or using recommendations from other neighboring UEs, and propagates the trust value of a particular neighboring UE in the neighborhood. Nevertheless, there are two main shortcomings: a) the trust values are computed based on local knowledge only (or a small portion of the entire network); and b) the trust values can be manipulated by the UE itself, or neighboring UEs during propagation.

C. ATTACK MODELS

There are *seven* main types of attacks against TRM.

A.1 *Sybil attacks:* The malicious nodes use more than one identity to confuse other nodes. They change to a fake identity and launch attack to avoid detection. Once detected, they change or impersonate others' identities and re-launch attacks. This process repeats until their intention is achieved (e.g., presenting themselves as trusted entities or sharing manipulated information about the operating environment).

A.2 *Crude attacks:* The malicious nodes forward incorrect information to the decision FC (i.e., the nodes forward manipulated information about themselves) in order to maximize their trust values about another neighboring node with the purpose of degrading the trust value of the node.

A.3 *Denial of service(DoS):* The malicious nodes prevent data forwarding and processing at legitimate nodes and applications. If the malicious nodes take control over the role of the controller(s), devices and applications in the data plane may experience a complete denial of service.

A.4 *Black hole attacks:* The malicious nodes suggest themselves as good packet forwarding candidates but drop received packets. For instance, when the malicious nodes gain control of the controller in the control plane, the forwarding function in the data plane can be manipulated, whereby devices and their routing tables can be manipulated with undesirable intention, particularly dropping packets/ data in the network.

A.5 *Routing attacks:* The malicious nodes change routing decisions, such as modifying the number of intermediate nodes to the destination node, and the actual destination address. The malicious controller(s) can modify the routing table so that data/ packets can be routed to manipulated destinations.

A.6 *Bad-mouthing attacks:* The malicious nodes make false recommendations about other nodes which affect decisions made. For instance, malicious nodes recommend a legitimate node as malicious to reduce its trust value, or recommend malicious nodes or itself as highly trusted nodes to increase their respective trust values.

A.7 *On-off attacks:* The malicious entities keep changing their behaviors (i.e., normal and malicious) from time to time to remain undetected. The malicious nodes remain undetected by confusing TRM with different behaviors at different points of time. So, at one time, a node is *On* (or malicious), while at another time, it is *Off* (or legitimate).

D. PERFORMANCE METRICS

This section presents various performance metrics evaluated in the TRM models.

M.1 *Misbehavior detection:* The network nodes or entities misbehave to gain self-benefit or influence other entities negatively. For instance, a node changes (impersonates) its identity to fool the network or other nodes, or manipulates the information about itself or others, to fulfill its malicious intention like suggesting itself as a good data forwarder. It increases with the detection of misbehaving entities in a collaboration.

M.2 *False/ true positive rate:* The false positive rate shows the false detection rate of legitimate entities instead of the malicious entities, while the true positive rate shows the correct detection rate of the malicious entities.

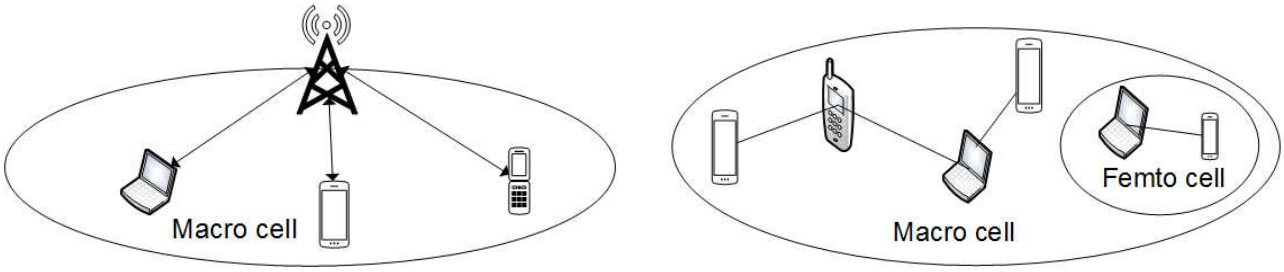
M.3 *Energy consumption:* The energy consumption of a network entity is caused by various actions (e.g., exchanging control messages and forwarding data packets to neighboring nodes), which increases with more attacks from malicious entities.

M.4 *Latency:* The end-to-end delay of packets/ information from a source to a destination affects the time period required for control message exchange, opinion dissemination, and trust value propagation.

E. CHALLENGES

C.1 *High heterogeneity:* The presence of distinctive net-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2984318, IEEE Access



(a) Centralized (b) Distributed

FIGURE 4: Traditional TRM models.

work entities and characteristics contributes to network heterogeneity. This includes *network architecture* that consists of macro and small cells, *access technologies* that consists of 5G, 4G, IEEE 802.11, *types of UEs* such as tablets, computers, and smart mobile devices, *characteristics* such as indoor and outdoor environment, as well as inband and outband transmissions. The challenge is to enable trust among heterogeneous devices and networks for collaboration to enhance network performance and perform network operations.

C.2 *High dynamicity:* The next-generation networks have ultra-dense and heterogeneous characteristics, and this leads to highly dynamic processes and data traffic that can change abruptly and unexpectedly. Due to the ultra-densification of network entities and devices, the behavior and the traffic are unexpectedly changing instantly, creating issues for controllers. The challenge is to predict, measure, and monitor the behaviors for evaluating and managing trust dynamically.

C.3 *High energy consumption:* Moving from the traditional tightly coupled planes to loosely coupled control and data planes promotes cooperation among networks and devices/ nodes that may be operating in a cellular or ad-hoc mode. Entities with different types of network cells (e.g., macro and small cells) can co-operate with each other, and different types of communications (e.g., direct communication in the cellular mode and D2D in the ad-hoc mode) can be used to share information to enhance network performance, such as meeting the capacity and coverage requirements. Network entities consume energy while sharing information in cooperation.

C.4 *High communication/ control overhead:* Since information is shared among participating entities in a co-operation, communication overhead can increase. The challenge is to minimize the communication/ message overhead throughout the collaboration process to maximize network performance.

IV. TRM FRAMEWORK

TRM is a framework for detecting malicious entities, including faulty, selfish, and malicious network entities, in a collaboration. In general, there are *six* main stages as shown in Table 3. More in-depth description about these stages for different schemes are presented in Section V.

1) Bootstrapping

Bootstrapping (or initialization) initializes the trust value of network entities during which their behaviors are unknown. The network entities may be assigned the same trust value, which is adjusted according to their behaviors as time goes by. For instance, in [26], nodes are initialized in three ways, either: a) neutral trust value; b) high trust value (i.e., trustworthy); or c) low trust value (i.e., untrustworthy). When the interaction with a network entity is infrequent, its trust value is updated infrequently, and so artificial (or dummy) beacons can be generated to increase the number of interactions so that its trust value reflects its behavior.

2) Information Gathering

Network entities gather information from neighboring network entities through:

- *Direct interaction information.* A network entity gathers information about a network entity through direct interaction with the network entity.
- *Indirect interaction information.* A network entity gathers information about a subject network entity through indirect interaction with other network entities. In other words, the information about the subject network entity is shared among network entities, and it is learned through information exchange. Nevertheless, at least a single network entity must learn about the subject network entity through direct interaction.

3) Information Dissemination

Network entities propagate direct and indirect interaction information with their neighboring network entities. The direct interaction information becomes indirect interaction information once it is propagated from one network entity to another. The information can be propagated either:

- a) *locally* (i.e., with neighboring nodes); or b) *globally* (i.e., with all nodes in the network).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2984318, IEEE Access

- a) *proactively* (i.e., every time interval); or b) *reactively* (i.e., upon the occurence of an event or a significant change to the network).

Nevertheless, malicious nodes can share:

- *positive information* whereby only good experiences about a subject network entity is shared, resulting in false praise attacks or ballot stuffing attacks [50].
- *negative information* whereby only bad experiences about a subject network entity is shared, resulting in bad-mouthing attacks [50].

4) Information Refinement

Network entities refine the direct and indirect interaction information. There are two considerations:

- *Credibility of information provider.* Since the indirect interaction information can be manipulated, the *credibility* of the information provider (i.e., network entity that provides the information) must be taken into consideration to prevent false reporting. For instance, different statistical distributions (e.g., Beta, Gaussian, Poisson, and Binomial distributions [52]) and deviation tests have been used to assess the credibility and consistency of the information provider. The deviation test enables a node to detect a malicious node if the difference between the indirect information about a subject node given by the malicious node and the direct information received by the node is greater than a threshold.
- *Recency of information.* Weight factor can be calculated because: a) the accuracy of the information reduces with the passage of time, and so newer information is given a higher weight factor compared to older information [22], [52]; b) the significance of the information should be taken into consideration (e.g., permanent link failure is more significant compared to temporary link failure), and more significant information is given a higher weight factor compared to less significant information. The weight factor can be subsequently used to calculate trust values.

5) Decision Making

Network entities calculate the trust and reputation values and separate legitimate and malicious network entities in order to choose the best possible network entities for interaction. Network entities, such as BS and FC, can aggregate trust and reputation values to provide collective and robust decisions. The decision can be based on the following methods:

- *Threshold* is used to determine trustworthiness. As an example, the trust value is higher (lower) than a threshold for a legitimate (malicious) network entity.
- *Ranking* is used to rank network entities based on their behaviors or trustworthiness. As an example, the neighboring nodes are ranked according to the accuracy of their channel sensing outcomes, which represent their trustworthiness. As another example, the individual nodes are ranked to select trusted routes for routing and packet transmission.
- *Weightage* is used to assign a weight to an aggregated information, which is received from network entities, based on the conditions of the network and operating environment. As an example, information received from different sensor nodes are combined in a FC or BS in order to provide a final judgment or summary on the condition of the network and operating environment being monitored.

6) Decision Dissemination

Network entities propagate the decisions made on a subject network entity (i.e., being legitimate or malicious) with their neighboring network entities either instantly or during the next interaction. Network entities, such as centralized entities (e.g., FC and BS), with high computational and storage capabilities can store the decisions and share them with other network entities, while network entities, such as sensors, with low computational and storage capabilities can disseminate the decisions (or trust values) to other nodes in distributed networks.

V. STATE OF THE ART

This section presents the state of the art, classified on the basis of common TRM techniques (see Section II-E). The description includes how the stages of the TRM framework (see Section IV and Table 3) are implemented in each state-of-the-art scheme. As TRM is at its infancy in the 5G networks, there are limited existing work in the literature. A qualitative comparison is given in Table 4.

A. TRM APPROACHES BASED ON RULES

This section presents *two* state-of-the-art schemes using the TRM approaches based on rules.

1) Energy-based Trust System for Detecting Sybil Attacks

Noor Alsaedi *et al.* [5] propose an energy-based multi-level trust scheme that detects malicious nodes at different levels (i.e., CH, CM, and BS) in clustered networks [28], [47]. The proposed scheme achieves the objectives of trust establishment (O.1), ensuring data reliability (O.2), and ensuring network scalability (O.3). The proposed scheme manages trust in a distributed manner (R.2) to countermeasure Sybil attacks (A.1). The proposed scheme addresses the challenges of high heterogeneity (C.1) in the presence of heterogeneous nodes (i.e., CM, CH and BS), and high dynamicity (C.2) whereby the behaviors of different network entities change with their available resources (i.e., residual energy) as time goes by.

The entities from different levels have different roles in

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2984318, IEEE Access

TABLE 3: TRM Framework

NO.	STAGE	DESCRIPTION
1	Bootstrapping	Initializes the trust value of network entities.
2	Information gathering	Network entities gather information from neighboring network entities through direct or indirect interaction.
3	Information dissemination	Network entities distribute direct and indirect local or global information to neighboring network entities in a proactive or reactive manner.
4	Information refinement	Network entities refine the received information based on the credibility of the information provider and the recency of the information.
5	Decision making	Network entities calculate trust values and separate legitimate and malicious network entities. Network entities, such as BS and FC, can aggregate trust values to provide collective decisions.
6	Decision dissemination	Network entities distribute decisions made on subject entities with neighboring network entities.

TABLE 4: Summary of objectives, characteristics, performance metrics, and challenges for different TRM schemes in 5G, which is the next-generation wireless network.

References	Year	Objectives			Characteristics		Performance Metrics				Challenges			
		O.1 Efficient trust between collaborating entities	O.2 Data reliability	O.3 Scalability	R.1 Centralized	R.2 Decentralized	M.1 Misbehavior detection	M.2 False/ true positives	M.3 Energy consumption	M.4 Latency	C.1 High Heterogeneity	C.2 High Dynamicity	C.3 High Energy consumption	C.4 Communication overhead
Xumin Huang *et al.* [21]	2017	×	×	×		×	×			×	×	×	×	×
Zhe Yang *et al.* [50]	2018	×	×	×		×	×			×	×	×	×	
Noor Alsaedi *et al.* [5]	2017	×	×	×		×		×	×		×	×		
Osama Alfarraj *et al.* [4]	2018	×	×	×		×	×	×	×	×	×	×	×	
Yang Yu *et al.* [53]	2016	×	×		×		×		×		×	×		×
Ying He *et al.* [20]	2018	×	×	×		×	×			×	×			×

detecting malicious nodes that launch Sybil attacks. There are two main stages. The first stage is *information gathering*, whereby the CMs sense and gather information about events in the operating environment (e.g., road accidents, fire, and natural disaster), and send information about themselves (e.g., their node IDs, geographical locations, and residual energy levels) and the events to the CH. The second stage is *decision making*, whereby the trust values are calculated by the CH at the cluster level. The CH maintains the node IDs, geographical locations, and residual energy of CMs in its storage. The CH identifies legitimate nodes in two steps. *Firstly*, the CH determines whether the information received from CMs is legimate or not by verifying their respective locations and node IDs stored in the CH. *Secondly*, the CH calculates the trust values of legitimate CMs based on their energy levels such that the trust value increases with the accuracy of the residual energy levels reported by the CMs. The total energy $E_{total} = E_{residual} + E_{consumed}$ is compared with the previously saved total energy E. Specifically, when $E \geq \Sigma(E_{total} + \lambda_1)$, where λ_1 is the change in the total energy of a CM, then the number of successful interactions with the CM is increased, otherwise the number of unsuccessful interactions with the CM is increased. Subsequently, the CH forwards the legitimate CMs' information to the BS. Next, the similar processes in the second stage is applied by BS to calculate trust values at the network level. So, the BS maintains the node IDs, geographical locations, and the residual energy levels of CHs in its storage, and identifies legitimate CHs.

The proposed scheme has shown to: a) increase misbehavior detection (M.1); b) improve the detection rate (M.2) of the Sybil node; and c) reduce energy consumption (M.3) by minimizing message exchanges between CMs and their

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2984318, IEEE Access

respective CHs.

2) Distributed Reputation Management in Edge Computing

Huang *et al.* [21], propose a distributed reputation management system (DREAMS) that manages reputation values at edge server in a vehicular network. In edge computing, edge servers have high computational capabilities and resources, and so they can collect, aggregate, and compute reputation values efficiently in order to identify and punish malicious vehicular nodes. The proposed scheme achieves the objective of trust establishment (O.1) whereby the edge server calculates and provides reputation values of the vehicular nodes, ensuring data reliability (O.2) whereby the vehicular nodes receive reliable information about an event, and ensuring network scalability (O.3) whereby the edge server provides trust values to all vehicular nodes. The proposed scheme manages reputation in a distributed manner (R.2) to countermeasure crude attacks (A.2), black hole attacks (A.4), and worm hole attacks. The proposed scheme addresses the challenges of high dynamicity (C.2) whereby the vehicular nodes communicate with the distributed edge server to receive quick response about the trustworthiness of the other vehicular nodes, and high energy consumption (C.3) whereby communication with the edge server, rather than the core network, reduces energy consumption.

There are two main components based on their locations: a) cloud server, which has higher computational capabilities and resources, is located far away from vehicular nodes; and b) edge servers are located at close proximity to vehicular nodes. The edge server can: a) provide computing services with improved network performance (e.g., lower end-to-end delay) to the vehicular nodes; and b) communicate and share information with the vehicular nodes. There are three main stages. The first stage is *information gathering*, whereby the edge server collects opinion metrics, which represents the legitimacy about a subject vehicular node that newly joins the network, from knowledgeable vehicular nodes. The second stage is *information refinement*, whereby the edge server uses the reputation value of the knowledgeable vehicular nodes to calculate a weight factor in order to adjust the opinion metrics given by the knowledgeable vehicular nodes. The reputation value of the knowledgeable vehicular nodes are obtained from the Cloud based on the historical and new reputation values. The third stage is *decision making*, whereby the edge server calculates the reputation value of the subject vehicular node using the weighted opinion metrics from the knowledgeable vehicular nodes. Knowledgeable vehicular nodes with reputation values lower than a threshold are considered malicious, and so they are either isolated or blacklisted. Subsequently, the reputation values are used to select vehicular nodes with high reputation values and to allocate resources to them.

DREAMS has shown to increase misbehavior detection (M.1) and reduce latency (M.4).

B. PROBABILISTIC TRM APPROACHES

This section presents *a* state of the art using the probabilistic TRM approach.

1) Efficient Trust Evaluation Scheme for Internet of Things

Yang Yu *et al.* [53], propose an efficient quantitative model for trust management in Internet of things (IoTs). The source node calculates and monitors the trust value of the next-hop and intermediate nodes based on various factors (e.g., whether the next-hop and intermediate nodes forward or drop its packets) in multi-hop networks. The proposed scheme achieves the objectives of trust establishment (O.1) whereby the source node calculates trust values of next-hop and intermediate nodes, ensuring data reliability (O.2) whereby packet integrity is monitored, and ensuring network scalability (O.3). The proposed scheme manages reputation in a distributed manner (R.2) to countermeasure crude (A.2), DoS (A.3), and black hole (A.4) attacks. The proposed scheme addresses the challenge of high energy consumption (C.3) whereby the exchange of control messages in a distributed environment is reduced.

There are two main stages. The first stage is *information gathering*, whereby the source node monitors the behavior of the relay node that has different forwarding characteristics (i.e., constant or variable forwarding and repetition rates causing different amount of delays). The second stage is *decision making*, whereby the source node calculates trust values based on the different forwarding characteristics using entropy. Entropy calculates different weight factors for different trust values to reduce the uncertainty of information. The direct trust value between node i and a next-hop node j is given by $T^D_{i,j} = \sum_{k=1}^{M} W_k T_k$, where the weight factor is $0 \leq W_k \leq 1$ and T_k is a forwarding characteristic of the entropy. The indirect trust values are gathered from neighboring nodes, and then aggregated with the direct trust value using the Dempster-Shafer theory [19], which merges information from independent (or different) nodes to minimize uncertainty.

The proposed scheme has shown to: a) increase malicious detection (M.1); b) reduce energy consumption (M.3); and c) minimize latency (M.4), whereby trust values are shared and communicated directly with next-hop or relay nodes rather than going through the BS.

C. ARTIFICIAL INTELLIGENCE-BASED TRM

This section presents *two* state of the art schemes using the artificial intelligence-based TRM approach.

1) Trusted Neighbor Node Selection for Secure Routing

Osama Alfarraj *et al.* [4], propose an activation function based on artificial neural networks, which use risk assessment and route probability, to calculate trust values of neighboring nodes in order to maintain a secured route between a source node and a destination node. The proposed scheme achieves

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2984318, IEEE Access

the objectives of trust establishment (O.1), ensuring data reliability (O.2), and ensuring network scalability (O.3). The proposed scheme manages trust in a distributed manner (R.2) to countermeasure DoS (A.3), black hole (A.4), and routing attacks (A.5). The proposed scheme addresses the challenges of high dynamicity (C.2), whereby there is a dynamic selection of trusted neighbors and less exchange of control messages (C.4), whereby it is a lightweight technique for constrained environment.

The proposed scheme has two main mechanisms in *decision making*. *Firstly*, the source node maintains the trust values of its neighboring nodes as time goes by so that malicious nodes can be identified and a new route can be discovered. The source node i calculates the trust value of its neighbor node j at time instant t is $S_{i,j}^t = F_{i,j}^t / R_{i,j}^t$, where $F_{i,j}^t$ represents the number of packets forwarded, and $R_{i,j}^t$ represents the number of packets arrived (or received). *Secondly*, the source node performs risk assessment on routes by calculating a probability, which takes account of the interaction quality (i.e., the number of communication) and response time (i.e., the time duration between sending a route request and receiving a route response). The risk assessment is performed after sending packets to the destination node whereby the trust value of the route is known, which is calculated by verifying the trustworthiness of each hop in the shortest route. Higher interaction quality indicates higher consistency of the quality of a route, while lower response time indicates lower packet loss caused by malicious nodes. A node is considered legitimate if it: a) has a trust value $S_{i,j}^t$ higher than the trust value of a route; b) has a trust value $S_{i,j}^t$ higher than a threshold; and c) has a residual energy level higher than half of its initial energy level. If a malicious node is identified in a route, the source node initiates a route discovery mechanism to establish a new secured route among the available routes.

The proposed scheme has shown to: a) increase misbehavior detection (M.1); b) reduce false positive (M.2); and c) reduce energy consumption (M.3).

2) Deep Q-Learning based Secure Social Networking in 5G

Ying He *et al.* [20], propose a social trust scheme for mobile social networks, which provide social relationship in social platforms (e.g., facebook and twitter) among users of various applications and services (e.g., content sharing). The proposed scheme achieves the objectives of trust establishment (O.1) based on social trust, ensuring data reliability (O.2) whereby data is monitored for manipulation, and ensuring network scalability (O.3). The proposed scheme manages reputation in a centralized manner (R.1) The proposed scheme addresses the challenges of high dynamicity (C.2) whereby the users have dynamic requirements, and high energy consumption (C.3) whereby the social trust values are exchanged with the nearest mobile edge server, which provides computational resources to close proximaty mobile users at the edge of the wireless mobile network.

The proposed scheme has two main stages. The first stage is *information gathering*, whereby a central entity (e.g., a BS, which is equipped with mobile edge computing (MEC) and cache, that provide high computational and storage capabilities at close physical proximity to users): a) uses the Bayesian inference model, which is a statistical method that computes the probability of receiving more evidences (or information) [34]. The Bayesian inference model is used to calculate the direct trust value T_i^D of a subject node i based on direct interaction experience (e.g., either forward, discard, or manipulated data); and b) uses the Dempster-Shafer approach, which combines evidences about a subject node from multiple nodes in order to improve the accuracy of the trust value of the subject node [19], [53]. The Dempster-Shafer approach is used to calculate indirect trust value T_i^I of a subject node i based on its direct trust value and indirect trust values gathered from neighboring nodes, which helps to identify malicious nodes that exhibit different behaviors towards different nodes. The second stage is *decision making*, whereby the BS calculates the trust value of a subject node i using $T_i = W \times T_i^D + (1 - W) \times T_i^I$ where $0 \leq W \leq 1$ represents a weight factor. The BS uses deep Q-learning (refer to [46]) to make decisions on which BS or D2D transmitter is assigned to serve a request (e.g., for a video) from a user based on various factors and characteristics, including the channel state (e.g., whether the channels are available or unavailable), version (e.g., whether the requested version is compatible and can be played at the requesting node), computational capabilities (e.g., whether the serving network entity, such as a BS or a node, is capable of computing, decoding, and sending the requested video), and trust value of a network entity. The trust value is used to make intelligent decision about the need for collaboration and communication for the required services (e.g., video content streaming).

The proposed scheme has shown to: a) increase malicious user detection (M.1); and b) reduce energy consumption (M.3) by receiving services from a close proximity D2D transmitter with high trust value.

D. BLOCKCHAIN-BASED TRM

This section presents *a* state of the art using the blockchain-based TRM approach.

1) Blockchain based Distributed Trust Managment in Vehicular Networks

Zhe Yang *et al.* [50], use blockchain among road side units (RSUs) for trust management. Blockchain is a peer-to-peer shared and distributed database that consists data and information in blocks [58]. RSUs are computing devices with higher resources and computational capabilities deployed at the road side [21], to collect information (e.g., geographical location and traffic condition) from vehicles. The proposed scheme achieves the objectives of trust establishment between vehicular nodes (O.1), ensuring data reliability (O.2) whereby the credibility of the messages are verified, and

ensuring network scalability (O.3) upon the detection and removal of malicious entities from the network. The proposed scheme manages reputation in a distributed manner (R.2) to countermeasure crude (A.2) and bad-mouthing (A.6) attacks. The proposed scheme addresses the challenges of high dynamicity (C.2) by managing trust at close proximity to RSU, high heterogeneity (C.1) by managing network entities with different computational capabilities on the road, and high energy consumption (C.3) by exchanging messages with the nearest RSU.

In general, a RSU receives opinions about a subject vehicular node from other vehicular nodes, computes the trust values of the subject vehicular node, and adds them to the block. There are three main stages. The first stage is *information gathering*, whereby RSUs collect messages about events and occurrences on the road from vehicular nodes. The second stage is *information refinement*, whereby RSUs calculate the credibility value of the vehicular nodes based on the distance between the vehicular nodes and the event, where a $+1$ value indicates a credible message, and a -1 value indicates a message with low trustworthiness. The third stage is *decision making*, whereby a RSU aggregates the creditability values from vehicular nodes to calculate a weighted offset trust value. This is necessary because the RSU may receive different number of $+1$ and -1 values. The RSUs elect a miner among themselves. The RSU with a higher number of stakes can find a nonce, which is a single-use random number used to calculate the hash of a block. The RSU with a hash value below a threshold, which is similar for all RSUs, wins the election. A miner has higher computational and storage capacities that can solve complex problems and perform complex tasks, such as *proof-of-work* that provides consensus strategies among miners while solving complex problems that require high computational capability, *proof-of-stake* that represents the sum of the stakes (or the amount of the trust value offsets), and *proof-of-capacity* that provides consensus strategies among peers to publish a block of trust value offsets [25], [58]. Upon receiving blocks from a miner, the RSU verifies the validity of the nonce, and then appends the block to the blockchain.

The proposed scheme has shown to: a) increase misbehavior detection (M.1) by verifying the credibility of the messages; b) reduce energy consumption (M.3) by using RSUs for complex calculations; and c) low latency (M.4) by communicating with nearby RSU rather than the core network.

VI. OPEN ISSUES AND FUTURE DIRECTIONS

This section presents open issues that can be further investigated in this research area. Collaboration is significant to various network functionalities, however at the same time, it opens doors to different security vulnerabilities. This section presents open issues, covering use of TRM to detect and remove malicious entities in collaboration schemes, which have not been investigated in the literature. Future directions of the use of TRM in our context are also presented.

A. ADDRESSING SECURITY VULNERABILITIES IN NETWORK VIRTUALIZATION

Network virtualization decouples a network into control and data layers to enable programmability, whereby requirements can be incorporated into networks elastically using 5G technologies, such as SDN and network slicing. The control layer consists of controllers that generate and exchange control messages comprised of commands and instructions, while the data layer consists of BSs, UEs and switches that receive control messages and follow the commands and instructions required for data forwarding. There are two main security advantages: a) *data traffic monitoring* in which controllers have global network information to determine whether a network entity is malicious or non-malicious; and b) *vulnerability robustness* in which the programmable nature of the network allows rapid response to security vulnerabilities and attacks.

Nevertheless, controllers must communicate and cooperate with each other to ensure the consistency of the network information in a multi-controller environment, including in core networks. Controllers can be manipulated by malicious entities and behave maliciously, such as providing manipulated policies for data forwarding and resource allocation, to reduce network performance. Two examples are presented. *Firstly*, a controller offers many open programmable interfaces to the application layer, which allows user applications to customize and modify the controller policies and operations according to the requirements and needs. This means that user applications can manipulate the interfaces, such as embedding malicious codes to the controllers that can affect the virtualized environment in a horizontal (i.e., other controllers in the same control layer) and vertical (i.e., the BSs, UEs, and switches in the data layer) manners. *Secondly*, the controllers in the control layer and the BSs, UEs, and switches in the data layer communicate with each other in order to exchange control messages; however, the communication can be intercepted by malicious entities that launch attacks either on the controllers, BSs, UEs, or switches. While the vulnerabilities of open programmable interfaces and the collaboration among controllers (or operators) have been investigated in [9] and [15], respectively, they have not been investigated in the 5G context. Research and investigation could be pursued to secure the network entities in the control and data layers to detect malicious entities.

B. ADDRESSING SECURITY VULNERABILITIES IN BEAMFORMING

With a higher frequency band (i.e., 2-300 GHz), mmWave provides a higher bandwidth to support an increased number of users. Nevertheless, mmWave has high penetration loss through walls and obstacles. Beamforming tracks a particular user's location and transmits packets to the user in a beam to reduce interference and penetration loss. BSs at different locations must exchange messages and cooperate with each other to focus beams towards their respective users while reducing interference. BSs can be manipulated by malicious

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2984318, IEEE Access

TABLE 5: Trust and reputation attacks

Authors	Year	TRM attacks							
		Sybil	Denial of service	Crude	Black hole	Routing	Worm hole	Bad-mouthing	White washing
Yang Yu, *et al.*	2016			×			×	×	
Ing-Re Chen, *et al.*	2016							×	×
Xumin Huang, *et al.*	2017			×			×		
Noor Alsaedi, *et al.*	2017	×			×	×			
V.Ram Prabha, *et al.*	2017			×	×	×		×	
Osama Alfarraj, *et al.*	2018		×		×				
Zhe Yang, *et al.*	2018					×	×		
Weizhi Meng, *et al.*	2018			×		×			
Ying He, *et al.*	2018			×			×		
Bilal Mughal, *et al.*	2018		×			×	×		×

entities and behave maliciously. Two examples are presented. *Firstly*, malicious entities generate and share manipulated information (e.g., the required beam and bandwidth, as well as the location, of a user) to increase interference and reduce spatial reuse. *Secondly*, malicious entities can intercept the location information in the communication among the BSs and exploit a user's privacy. While the vulnerabilities of beamforming have been investigated in [18] and [57], respectively, they have not been investigated in the 5G context. Research and investigation could be pursued to detect malicious entities and secure beamforming using security measures including TRM.

C. ADDRESSING SECURITY VULNERABILITIES IN ACCESSING MMWAVE FREQUENCY BANDS

Using mmWave transmission can help to access underutilized channels in the high frequency bands in order to increase network capacity, which has been limited by the fixed traditional spectrum allocation policy. This helps to cater for the increasing data traffic under ultra-densification scenario in 5G. Each network entity must sense for channel availability. Cooperation enables network entities to share and exchange channel information (e.g., channel availability) among network entities so that they can make intelligent decisions on channel access in an autonomous manner. Nevertheless, network entities and channel sensing outcomes can be manipulated by malicious entities and behave maliciously to reduce network performance. As an example, malicious entities generate and share manipulated channel information (e.g., channel availability). This causes network entities to access unavailable channels or miss opportunities to access available channels. Consequently, this can increase interference, as well as reduce bandwidth and spatial reuse. While the vulnerabilities of the access to mmWAve frequency bands have been investigated in [59] and [48], respectively, they have not been investigated using TRM in the 5G context. Research and investigation could be pursued to detect malicious entities and secure dynamic channel access in mmWave frequency bands in order to secure channel access in an intelligent and collaborative manner.

D. USING SUBJECTIVITY OF DATA IN TRM

The subjectivity of data provides opinion about a network entity based on one's personal experience and recommendation while interacting with the network entity. Hence, a network entity's opinion about another network entity may differ dependent on the perception generated from an interaction, which may or may not provide accurate recommendations. Malicious entities can use subjectivity for their malicious benefits. As an example, if a subject node i has a high trust value, and a recommender node j provides false recommendation or negative opinion to reduce the subject node i's trust value. Hence, assigning accurate weight to opinion or recommendation affects the trust evaluation process. A node can use statistical theorems and mathematical models to reduce the misleading effect of inaccurate recommendations in trust evaluation. In [55], a node uses a regression technique to evaluate the recommendations received from neighboring nodes, and an alignment mechanism to counteract biases in the recommendations substantially. The aligned recommendations are propagated among neighboring nodes so that the effect of inaccurate recommendations can be minimized. In [3], a node uses triangular fuzzy numbers [43], to represent the weights of different trust criteria used to evaluate a trust value so that more accurate criteria are given higher weight values. Despite the abundance of literature on trust and reputation, the subjectivity issue has not been well investigated [27], particularly in the 5G context. Specifically, mechanisms to address the effect of ultra-densification, high heterogeneity, and high variability, to the accuracy of recommendations

as a result of subjectivity is yet to be discovered. Research could be pursued to investigate statistical theorems and mathematical models for trust evaluation and management in order to manage subjectivity and its effects.

E. ADDRESSING SECURITY VULNERABILITIES IN NETWORK SLICING

Network slicing separates resources into various parts (or slices) to meet different user and network requirements on resources and services (e.g., the RAN requirements for remote surgery and driverless vehicles). The requirements can be incorporated into networks elastically using 5G technologies, such as SDN and network function virtualization [14], [56]. The controller manages and updates the slices on the fly to fulfill the specific requirements. Controllers must communicate and cooperate with each other to ensure the consistency of network information in a multi-controller environment. Controllers can be manipulated by malicious entities and behave maliciously, such as providing manipulated policies for resource allocation, to reduce network performance. Research could be pursued to secure network slicing, particularly the controllers that manage resources in the control layer.

F. ADDRESSING QUANTITATIVE ANALYSIS COMPLICATIONS

Due to the different characteristics and features of TRM schemes proposed in the literature, as well as the underlying network initialization settings and topologies, there is lack of study on qualitative comparison among the TRM schemes. The characteristics of 5G networks, including ultra-densification, high heterogeneity, and high variability, contribute to the diversity of the investigations made in this research topic. While traditional security schemes, such as cryptography [2], [12], are mathematically tractable, the TRM schemes proposed in the literature [20], [31], that are based on artificial intelligence approaches are not mathematically tractable. This means that qualitative comparison among the security schemes can be non-mathematically tractable, such as using Monte Carlo simulation, yet the investigation must be comprehensive to minimize security vulnerability. Further research could be pursued to conduct a fair qualitative comparison among the schemes under a comprehensive set of network initialization settings and topologies.

G. FUTURE DIRECTIONS

5G access network is expected to be: a) highly dynamicity, whereby the network requirements of the network entities change dynamically and are unpredictable; and b) highly heterogeneous, whereby the network entities have different natures and characteristics. High dynamicity and heterogeneity increase security vulnerabilities due to the complexity of managing the network. We present two future directions of research in TRM applied to 5G access networks as follows:

1) Hybrid TRM Framework

Centralized and distributed TRM schemes [4], [5], [53], have been proposed to handle dynamicity and heterogeneity, respectively. The centralized TRM schemes are embedded in a central entity, such as FC, BS, and CH, to manage and disseminate trust values among network entities in order to assess their behaviors in a centralized manner. On the other hand, the distributed TRM schemes are embedded in different network entities, such as nodes and RSUs, to manage and exchange trust values among themselves. Nevertheless, due to the highly dynamic and heterogenous 5G network scenarios, the traditional centralized and distributed TRM approaches are insufficient. The centralized approach requires network-wide information which may not be able to cater for real-time response; while the distributed approach requires local information only which may not be optimal for making network-wide decision. In addition, the centralized approach can handle low dynamic aspects, while the distributed approach can handle highly dynamic aspects. Hence, a hybrid framework that incorporates both centralized and distributed approaches is needed to cater for dynamic schemes (i.e., from low to high dynamicity) and heterogeneous schemes (i.e., from real-time to delay tolerant schemes) that requires different levels of responses. Moreover, the hybrid framework can address security vulnerabilities at both local (i.e., node) and global (i.e., BS) levels of a 5G access network. Hence, more investigations on a hybrid framework for TRM is expected in 5G access networks.

2) Application of Artificial Intelligence to TRM

Artificial intelligence approaches, such as reinforcement learning [20] and the Bayesian approach, have been incorporated into TRM to learn and detect malicious entities, as well as to make security decisions, with increased accuracy in the presence of dynamic operating environment. Dynamicity changes the operating environment that warrants different policy (or sets of actions) for achieving optimal network performance. Nevertheless, traditional artificial intelligence approaches may not be sufficiently efficient and flexible to cater. While the centralized approach (e.g., embedded in BS) can use more complex artificial intelligence approaches, such as deep learning [29], [46] to handle complex network scenarios, the distributed approach (e.g., embedded in UEs) can only use less complex artificial intelligence approaches. Meanwhile, the malicious entities can also use artificial intelligence approaches to learn the best strategy to launch attacks. Hence, more investigations on the use of artificial intelligence to TRM, as well as to address artificial intelligence-based attacks, are expected in 5G access networks.

VII. CONCLUSION

This article presents a review on the limited works on trust and reputation management (TRM) in 5G. 5G is envisioned to address the limitations of traditional cellular networks (i.e., low network capacity, high latency, inefficient data forward-

ing, and low scalability) and to cater for the characteristics of next-generation network scenarios (i.e., high heterogeneity, ultra-densification, and high variability). Collaboration has become indispensable to support important functions in 5G, particularly dynamic channel access, device-to-device communication, network virtualization, and coordinated multi-point in order to enhance spectral efficiency, network capacity, QoS performance (e.g., latency), and energy efficiency. Nevertheless, collaboration is susceptible to security vulnerabilities and attacks, such as Sybil, crude, denial of service, black hole attacks, and so on. TRM has been proposed to establish trust among collaborating entities, as well as to improve data reliability and scalability. Nevertheless, TRM must address challenges brought about by 5G, including high heterogeneity, dynamicity, energy consumption, and overhead. Traditional TRM must be enhanced to be applied in 5G networks. This article discusses how TRM can improve 5G networks, and open research opportunities. Future investigation could be pursued to apply TRM to enhance security in 5G networks, including channel access and sharing, beamforming, D2D communication, and network virtualization. In addition, future investigation could also be pursued to improve TRM approaches, such as extending the centralized and distributed approaches to the hybrid approach, and to use more advanced learning approaches, such as deep learning. Certainly, this article has laid a solid foundation and opened up new research interests in this area.

REFERENCES

[1] M. Agiwal, A. Roy, and N. Saxena. Next Generation 5G Wireless Networks: A Comprehensive Survey. IEEE Communications Surveys & Tutorials, 18(3):1617–1655, 2016.

[2] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov. Overview of 5G Security Challenges and Solutions. IEEE Communications Standards Magazine, 2(1):36–43, Mar 2018.

[3] A. I. A. Ahmed, S. Khan, A. Gani, S. H. A. Hamid, and M. Guizani. Entropy-based Fuzzy AHP Model for Trustworthy Service Provider Selection in Internet of Things. In 2018 IEEE 43rd Conference on Local Computer Networks (LCN). IEEE, Oct 2018.

[4] O. AlFarraj, A. AlZubi, and A. Tolba. Trust-based Neighbor Selection using Activation Function for Secure Routing in Wireless Sensor Networks. Journal of Ambient Intelligence and Humanized Computing, Jun 2018.

[5] N. Alsaedi, F. Hashim, A. Sali, and F. Z. Rokhani. Detecting sybil attacks in clustered wireless sensor networks based on energy trust system (ETS). Computer Communications, 110:75–82, Sep 2017.

[6] R. Bajracharya, R. Shrestha, R. Ali, A. Musaddiq, and S. W. Kim. LWA in 5G: State-of-the-Art Architecture, Opportunities, and Research Challenges. IEEE Communications Magazine, 56(10):134–141, Oct 2018.

[7] J. Bennaceur, H. Idoudi, and L. A. Saidane. Trust Management in Cognitive Radio Networks: A Survey. International Journal of Network Management, 28(1):e1999, Sep 2017.

[8] T. Biermann, L. Scalia, C. Choi, H. Karl, and W. Kellerer. CoMP Clustering and bBackhaul Limitations in Cooperative Cellular Mobile Access Networks. Pervasive and Mobile Computing, 8(5):662–681, Oct 2012.

[9] E. Bulut and A. Gosain. Mobile Core Network Redimensioning for Efficient Resource Utilization. In 2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, May 2017.

[10] S. A. Busari, K. M. S. Huq, S. Mumtaz, L. Dai, and J. Rodriguez. Millimeter-Wave Massive MIMO Communication for Future Wireless Systems: A Survey. IEEE Communications Surveys & Tutorials, 20(2):836–869, 2018.

[11] Q. Cui, H. Wang, P. Hu, X. Tao, P. Zhang, J. Hamalainen, and L. Xia. Evolution of Limited-Feedback CoMP Systems from 4G to 5G: CoMP Features and Limited-Feedback Approaches. IEEE Vehicular Technology Magazine, 9(3):94–103, Sep 2014.

[12] D. Fang, Y. Qian, and R. Q. Hu. Security for 5G Mobile Wireless Networks. IEEE Access, 6:4850–4874, 2018.

[13] R. Fantacci and D. Marabissi. Cognitive Spectrum Sharing: An Enabling Wireless Communication Technology for a Wide Use of Smart Systems. Future Internet, 8(4):23, May 2016.

[14] X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina. Network Slicing in 5G: Survey and Challenges. IEEE Communications Magazine, 55(5):94–100, May 2017.

[15] D. Goltzsche, S. Rusch, M. Nieke, S. Vaucher, N. Weichbrodt, V. Schiavoni, P.-L. Aublin, P. Cosa, C. Fetzer, P. Felber, P. Pietzuch, and R. Kapitza. EndBox: Scalable Middlebox Functions Using Client-Side Trusted Execution. In 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). IEEE, Jun 2018.

[16] A. Gupta and R. K. Jha. A Survey of 5G Network: Architecture and Emerging Technologies. IEEE Access, 3:1206–1232, 2015.

[17] M. A. Habibi, M. Nasimi, B. Han, and H. D. Schotten. A Comprehensive Survey of RAN Architectures Toward 5G Mobile Communication System. IEEE Access, 7:70371–70421, 2019.

[18] J. Harbin and P. Mitchell. Reputation Routing to Avoid Sybil Attacks in Wireless Sensor Networks using Distributed Beamforming. In 2011 8th International Symposium on Wireless Communication Systems. IEEE, Nov 2011.

[19] Y. He, F. R. Yu, Z. Wei, and V. Leung. Trust Management for Secure Cognitive Radio vehicular Ad hoc Networks. Ad Hoc Networks, 86:154–165, Apr 2019.

[20] Y. He, F. R. Yu, N. Zhao, and H. Yin. Secure Social Networks in 5G Systems with Mobile Edge Computing, Caching, and Device-to-Device Communications. IEEE Wireless Communications, 25(3):103–109, Jun 2018.

[21] X. Huang, R. Yu, J. Kang, and Y. Zhang. Distributed Reputation Management for Secure and Efficient Vehicular Edge Computing and Networks. IEEE Access, 5:25408–25420, 2017.

[22] F. Ishmanov, A. S. Malik, S. W. Kim, and B. Begalov. Trust management system in wireless sensor networks: design considerations and research challenges. Transactions on Emerging Telecommunications Technologies, 26(2):107–130, Jun 2013.

[23] A. Jøsang, R. Ismail, and C. Boyd. A Survey of Trust and Reputation Systems for Online Service Provision. Decision Support Systems, 43(2):618–644, Mar 2007.

[24] V. Jungnickel, K. Manolakis, W. Zirwas, B. Panzner, V. Braun, M. Lossow, M. Sternad, R. Apelfrojd, and T. Svensson. The role of small cells, coordinated multipoint, and massive MIMO in 5G. IEEE Communications Magazine, 52(5):44–51, May 2014.

[25] J. Kang, Z. Xiong, D. Niyato, P. Wang, D. Ye, and D. I. Kim. Incentivizing Consensus Propagation in Proof-of-Stake Based Consortium Blockchain Networks. IEEE Wireless Communications Letters, 8(1):157–160, Feb 2019.

[26] O. Khalid, S. U. Khan, S. A. Madani, K. Hayat, M. I. Khan, N. Min-Allah, J. Kolodziej, L. Wang, S. Zeadally, and D. Chen. Comparative Study of Trust and Reputation Systems for Wireless Sensor Networks. Security and Communication Networks, 6(6):669–688, Jul 2012.

[27] J. Khan and S. Lee. Implicit User Trust Modeling Based on User Attributes and Behavior in Online Social Networks. IEEE Access, 7:142826–142842, 2019.

[28] T. Khan, I. Ahmad, W. Aman, I. Azam, Z. A. Khan, U. Qasim, S. Avais, and N. Javaid. Clustering Depth Based Routing for Underwater Wireless Sensor Networks. In 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA). IEEE, Mar 2016.

[29] Y. LeCun, Y. Bengio, and G. Hinton. Deep Learning. Nature, 521(7553):436–444, May 2015.

[30] Q. Li, A. Malip, K. M. Martin, S.-L. Ng, and J. Zhang. A Reputation-Based Announcement Scheme for VANETs. IEEE Transactions on Vehicular Technology, 61(9):4095–4108, Nov 2012.

[31] M. H. Ling and K.-L. A. Yau. Reinforcement Learning-based Trust and Reputation Model for Cluster head Selection in Cognitive Radio Networks. In The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014). IEEE, Dec 2014.

[32] J. Lopez, R. Roman, I. Agudo, and C. Fernandez-Gago. Trust Management Systems for Wireless Sensor Networks: Best Practices. Computer Communications, 33(9):1086–1093, Jun 2010.

[33] W. Meng, K.-K. R. Choo, S. Furnell, A. V. Vasilakos, and C. W. Probst. Towards Bayesian-Based Trust Management for Insider Attacks in Healthcare Software-Defined Networks. IEEE Transactions on Network and Service Management, 15(2):761–773, Jun 2018.

[34] B. K. Mughal, S. Hameed, and B. Hameed. Isolating Malicious Controller(s) In Distributed Software-Defined Networks with Centralized Reputation Management. International Journal of Future Generation Communication and Networking, 11(5):11–26, Sep 2018.

[35] V. R. Prabha and P. Latha. Fuzzy Trust Protocol for Malicious Node Detection in Wireless Sensor Networks. Wireless Personal Communications, 94(4):2549–2559, Sep 2016.

[36] T. S. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G. N. Wong, J. K. Schulz, M. Samimi, and F. Gutierrez. Millimeter Wave Mobile Communications for 5G Cellular: It Will Work! IEEE Access, 1:335–349, 2013.

[37] J. Ren, Y. Zhang, Q. Ye, K. Yang, K. Zhang, and X. S. Shen. Exploiting Secure and Energy-Efficient Collaborative Spectrum Sensing for Cognitive Radio Sensor Networks. IEEE Transactions on Wireless Communications, 15(10):6813–6827, Oct 2016.

[38] K. Rina, S. Nath, N. Marchang, and A. Taggu. Can Clustering be Used to Detect Intrusion During Spectrum Sensing in Cognitive Radio Networks? IEEE Systems Journal, 12(1):938–947, Mar 2018.

[39] S. Sekander, H. Tabassum, and E. Hossain. Multi-Tier Drone Architecture for 5G/B5G Cellular Networks: Challenges, Trends, and Prospects. IEEE Communications Magazine, 56(3):96–103, Mar 2018.

[40] Z. Shu, J. Wan, D. Li, J. Lin, A. V. Vasilakos, and M. Imran. Security in Software-Defined Networking: Threats and Countermeasures. Mobile Networks and Applications, 21(5):764–776, Jan 2016.

[41] D. Soldani and A. Manzalini. Horizon 2020 and Beyond: On the 5G Operating System for a True Digital Society. IEEE Vehicular Technology Magazine, 10(1):32–42, Mar 2015.

[42] G. I. Tsiropoulos, A. Yadav, M. Zeng, and O. A. Dobre. Cooperation in 5G HetNets: Advanced Spectrum Access and D2D Assisted Communications. IEEE Wireless Communications, 24(5):110–117, Oct 2017.

[43] G. G. Udo. Using Analytic Hierarchy Process to Analyze the Information Technology Outsourcing Decision. Industrial Management & Data Systems, 100(9):421–429, Dec 2000.

[44] K. Ullah, I. Rashid, H. Afzal, W. Iqbal, Y. A. Bangash, and H. Abbas. SS7 Vulnerabilities - A Survey & Implementation of Machine Learning Vs Rule Based Filtering for Detection of SS7 Network Attacks. IEEE Communications Surveys & Tutorials, 2020.

[45] J. Wang, I.-R. Chen, J. J. Tsai, and D.-C. Wang. Trust-based Cooperative Spectrum Sensing against SSDF Attacks in Distributed Cognitive Radio Networks. In 2016 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR 2016). IEEE, May 2016.

[46] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, and C. Wang. Machine Learning and Deep Learning Methods for Cybersecurity. IEEE Access, 6:35365–35381, 2018.

[47] L. Xu, R. Collier, and G. M. P. O'Hare. A Survey of Clustering Techniques in WSNs and Consideration of the Challenges of Applying Such to 5G IoT Scenarios. IEEE Internet of Things Journal, 4(5):1229–1249, Oct 2017.

[48] Q. Xue, P. Zhou, X. Fang, and M. Xiao. Performance Analysis of Interference and Eavesdropping Immunity in Narrow Beam mmWave Networks. IEEE Access, 6:67611–67624, 2018.

[49] Z. Yan, P. Zhang, and A. V. Vasilakos. A Security and Trust Framework for Virtualized Networks and Software-defined Networking. Security and Communication Networks, 9(16):3059–3069, Mar 2015.

[50] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung. Blockchain-Based Decentralized Trust Management in Vehicular Networks. IEEE Internet of Things Journal, 6(2):1495–1505, Apr 2019.

[51] S. Yao, Z. Li, J. Guan, and Y. Liu. Stochastic Cost Minimization Mechanism based on Identifier Network for IoT Security. IEEE Internet of Things Journal, 2019.

[52] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato. A Survey of Trust and Reputation Management Systems in Wireless Communications. Proceedings of the IEEE, 98(10):1755–1772, Oct 2010.

[53] Y. Yu, Z. Jia, W. Tao, B. Xue, and C. Lee. An Efficient Trust Evaluation Scheme for Node Behavior Detection in the Internet of Things. Wireless Personal Communications, 93(2):571–587, Oct 2016.

[54] K. Zeb, X. Zhang, and Z. Lu. High Capacity Mode Division Multiplexing Based MIMO Enabled All-Optical Analog Millimeter-Wave Over Fiber Fronthaul Architecture for 5G and Beyond. IEEE Access, 7:89522–89533, 2019.

[55] L. Zeynalvand, J. Zhang, T. T. Luo, and S. Chen. MASA: Multi-Agent Subjectivity Alignment for Trustworthy Internet of Things. In 2018 21st International Conference on Information Fusion (FUSION). IEEE, Jul 2018.

[56] H. Zhang, N. Liu, X. Chu, K. Long, A.-H. Aghvami, and V. C. M. Leung. Network Slicing Based 5G and Future Mobile Networks: Mobility, Resource Management, and Challenges. IEEE Communications Magazine, 55(8):138–145, Aug 2017.

[57] X. Zhang, X. Zhou, and M. R. McKay. Enhancing Secrecy With Multi-Antenna Transmission in Wireless Ad Hoc Networks. IEEE Transactions on Information Forensics and Security, 8(11):1802–1814, Nov 2013.

[58] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In 2017 IEEE International Congress on Big Data (BigData Congress). IEEE, Jun 2017.

[59] Y. Zhu, L. Wang, K.-K. Wong, and R. W. Heath. Secure Communications in Millimeter Wave Ad Hoc Networks. IEEE Transactions on Wireless Communications, 16(5):3205–3217, May 2017.

ISRAR AHMAD received the B.S. degree (Hons.) in information technology from The University of Agriculture (IBMS), Peshawar in 2014 and M.S. degree in information security from the COMSATS University, Islamabad in 2017. He is currently pursuing Ph.D. degree from Sunway University, Malaysia. He is a reseacher and industry based academician in information security, privacy, artificial intelligence, wireless networks and communications.

KOK-LIM ALVIN YAU (M'08) received the B.Eng. degree (Hons.) in electrical and electronics engineering from Universiti Teknologi Petronas, Malaysia, in 2005, the M.Sc. degree in electrical engineering from the National University of Singapore in 2007, and the Ph.D. degree in network engineering from the Victoria University of Wellington, New Zealand, in 2010.

He is currently a Professor with the Department of Computing and Information Systems, Sunway University. He is also a Researcher, a Lecturer, and a Consultant in cognitive radio, wireless networks applied artificial intelligence, and reinforcement learning. He serves as a TPC member and a reviewer for major international conferences, including ICC, VTC, LCN, GLOBECOM, and AINA. He was a recipient of the 2007 Professional Engineer Board of Singapore Gold Medal for being the best graduate of the M.Sc. degree in 2006/2007.

Dr. Yau serves as an Associate Editor for the IEEE ACCESS, an Editor of the KSII Transactions on Internet and Information Systems, a Guest Editor of the Special Issues of IEEE ACCESS, IET Networks, IEEE Computational Intelligence Magazine, and the Springer Journal of Ambient Intelligence and Humanized Computing, and a regular reviewer for over 20 journals, including the IEEE journals and magazines, the Ad Hoc Networks, the IET Communications, and others. He also served as the General Co-Chair of the IET ICFCNA'14 and the Co-Chair of the Organizing Committee of the IET ICWCA'12.

MEE HONG LING received the B. Sc. degree (Hons.) in computer and mathematical studies from Oxford Brookes University, U.K., and the M. Sc. degree in data engineering (computer science) from Keele University, U.K., and the Ph.D. degree in computing from Sunway University, Malaysia. She lectures with the Department of Computing and Information Systems, Sunway University. Her research interests are in the areas of security, cognitive radio networks, and artificial intelligence.

SYE LOONG KEOH is an Associate Professor in the School of Computing Science, University of Glasgow (UofG, Singapore campus) and the Director of Research Programmes in UofG Singapore. He holds a Ph.D. in computing science from Imperial College London. Prior to joining Glasgow, he was a Senior Scientist at Philips Research Eindhoven, The Netherlands. His areas of expertise include cyber security for Internet of Things (IoT), lightweight security systems for cyber-physical systems, and policy-based security management for pervasive and distributed systems.

He leads the cyber-security research activities in UofG Singapore where he has designed several lightweight authentication protocols and key management schemes for IoT, building management and industrial control systems. More recently, he is researching on new techniques for securing end-to-end communication and ensuring data provenance in IoT environment. While working at Philips Research, he was responsible for standardizing Marlin Digital Rights Management (DRM) technology for content protection, and lightweight security protocols for Philips's IoT-based lighting systems.