Security Issues in Multi-hop Device-to-device Communication Networks - Secure Routing Protocols Solution

Yimin Lv
750 Test Range, China State Shipbuilding Corporation Limited, Kunming, Yunnan, China
Email: 1443612254@qq.com

Abstract. As one of the key technologies of fifth-generation mobile communication, device-to-device communication technology can not only realize direct communication between neighboring devices, but also reduce the delay of local services provided to users and increase the communication rate. Nevertheless, the special structure of the device-to-device communication network makes it more vulnerable to attacks from inside and outside the network. This paper summarizes the security issues faced by device-to-device communication networks, analyzes the secure routing designed for different types of attacks, and discusses future research directions.

1. Introduction
The fifth-generation mobile communication technology (5G) was officially named IMT-2020 by the International Telecommunication Union (ITU) in June 2015, which main application scenarios include mobile broadband, large-scale machine communications (e.g. smart cities, smart homes) and high-reliable and low-latency communications (e.g. autonomous vehicles, industrial automation, augmented reality, etc.) [1]. In order to meet the above application scenarios, 5G networks integrate multiple types of wireless access transmission technologies, including traditional cellular networks, wireless local area networks (Wi-Fi), wireless sensor networks (WSN), small base stations, and device-to-device communications (D2D), etc., and control these wireless networks through a unified core network to provide ultra-high-speed and ultra-low-latency user experience and consistent seamless services in multiple scenarios.

Device-to-device communication network (D2D) is one of the key technologies of 5G. Device-to-device (D2D) communication technology can realize communication between adjacent and non-adjacent devices without core equipment such as base stations, and reduce the data flow through the network and increase the capacity of the communication system. Therefore, the D2D communication technology can be used as a supplement to cellular communication networks in remote mountainous areas or airports and other places where network infrastructure is lacking, and provide emergency communication for devices in the event of sudden disasters that cause network infrastructure damage. In addition, the D2D communication industry also can provide local services for devices in situations such as community and shopping mall promotions.

There are many applications of the device-to-device communications, such as completing interactions in the Internet of Vehicles through the D2D communications; building ad hoc networks based on multi-hop D2D communication networks; combining of cellular network and the D2D networks to form the heterogeneous networks, etc. [1]. Up to now, the main research directions of D2D...
as follows: (i) Device discovery and session establishment; (ii) Link performance issues; (iii) Resource allocation issues, including interference management and Qos allocation [2].

2. Security Issues in Multi-hop Device-to-device Communication Networks

Although the D2D communications have widely application scenarios, it is more difficult to guarantee the security and privacy of spontaneous and self-management users in D2D networks compared with the traditional centralized environment [3]. Secure wireless communication should have authenticity, privacy, confidentiality, integrity and availability. Security and privacy are equally important in D2D networks, though there are a certain contradiction between them.

With the increase in the scale of the D2D communication network and the continuous complexity of the network structure, the single-hop D2D network will not be able to meet the communication requirements of the device, as thus multi-hop D2D communication network is one of the development directions of D2D communication technology.

Unfortunately, multiple types of attacks exist in ad hoc networks based on multi-hop D2D communication networks. Attacks can be divided into internal attacks and external attacks from the location of the attack. Attacks sent by a node are internal attacks, and attacks sent from outside the node are external attacks. According to the attack mode, attacks can be divided into active attacks and passive attacks. Passive attacks often manifest as eavesdropping, without affecting network communications [4]. Active attacks include Denial-of-services (DoS) attacks, black hole attacks, gray hole attacks, wormhole attacks, and selfish node attacks. The specific types attacks are shown in Figure 1. DoS attacks have the characteristics of strong concealment and low cost, which can occupy network bandwidth through message bombing and cause severe congestion or even paralysis of the wireless distributed network. A large number of selfish nodes may cause the network to fail to provide packet forwarding services normally.

| DoS attacks                                      | Computer network broadband attacks, connectivity attacks |
|-------------------------------------------------|--------------------------------------------------------|
| black hole attacks                              | The malicious nodes send out wrong routing information to attract data packets, and then discard the data packets. |
| gray hole attacks                               | The malicious nodes discard a part of the data packets. |
| wormhole attacks                                | Multiple malicious nodes maintain illegal links to transmit data packets to malicious nodes outside the normal routing. |
| selfish nodes                                   | Selfish nodes evade participating in routing services by tampering with routing protocols, or forwarding data packets, or selectively forwarding data packets for the sake of saving its own energy. |

Figure 1. The specific types of active attacks.

Malware attack is also a common type of attack in ad hoc networks. Malware may automatically deduct user charges and read the sensors installed on the smart devices to steal the user's password and other information. The formation of the malware industry was no later than 2013 [5].

In recent years, with the development of technology, more and more people use smart terminals to complete electronic funds transfer (electronic funds transfer, EFT), so the smart terminals usually contain a large number of private information like bank accounts and passwords [6]. Multi-hop D2D communications usually use the technologies such as Near Field Communication (NFC), Ultra-Wide Band (UWB), Bluetooth, ZigBee, WiFi or LTE [3]. Malware can quickly spread among smart terminals through multimedia messaging systems (MMS) such as Bluetooth or Cabir. Therefore, malware attacks will inevitably bring huge potential security risks to the D2D communications.

3. Security Problem Solution
The security requirements in D2D communication can be divided into the following categories: (i) Identity verification and authorization; (ii) Availability and reliability; (iii) Non-repudiation; (iv) Secure routing and transmission; (v) Confidentiality; (vi) Integrity. Corresponding, the existing security solutions are divided into five areas: (i) key management; (ii) identity verification; (iii) confidentiality and integrity; (iv) availability and reliability; (v) secure routing and transmission.

Compared with traditional single-hop D2D communication networks, ad hoc networks composed of multi-hop D2D usually do not have network infrastructure (e.g. base stations) which provides encryption and other security resources, thus, we focus on the secure routings which resist attacks. To realize the safe routing of data packets, the data packet routing algorithm can be directly optimized, or other means, such as malicious node detection, can be used to ensure the safe transmission of data packets.

4. Secure Routing Solution in Multi-hop Device-to-device Communication Networks

In fact, the security solutions are mutually permeable, for example, the author of [7] proposed an energy-saving AODV routing protocol that provides end-to-end routing authentication with digital signature authentication. Multi-hop D2D network can be regarded as an ad hoc network based on multi-hop D2D, so multi-hop D2D network routing protocol usually refers to ad hoc network routing protocol.

4.1. Multi-hop D2D Network Routing Protocol

According to the operating mechanism, ad hoc routing protocols can be divided into three categories: active routing protocols (table-driven routing protocols), passive routing protocols (reactive routing protocols) and hybrid routing protocols [8]. According to different network structures, ad hoc network routing protocols can be divided into flat routing protocols and hierarchical routing protocols.

Most of the existing ad hoc network routing protocols are improvements and enhancements to the classic ad hoc network routing protocols. The enhancement indicators include network quality of service (QoS) and survivability. For example, the literature [9] used selective routing based on the SNR threshold in the reverse routing mechanism and proposed an AODV SNR-SR selective routing protocol; the author of [10] proposed a selective ad hoc on-demand multipath distance vector algorithm based on load balancing, which is an enhanced protocol of AODV.

At present, most of the research on secure routing in multi-hop D2D communication networks is also an improvement on the classic ad hoc routing protocol, and is aimed at specific attack methods.

4.2. Secure Routing Protocols against DoS Attacks

DoS attacks often come from neighboring nodes of the node, so Hash function and other means to verify the source of data packets can resist DoS attacks in multi-hop D2D networks, as the literature [11] proposed an improved protocol of ALERT protocol using pseudonym of location of node technique to resist DoS attacks.

Scholars also use node trust to detect malicious nodes so as to resist DoS attacks. The author of [12] proposed an enhanced protocol of AODV that can resist DoS attacks. The protocol sends pseudo data packets generated by the source node to the target node to calculate the trust method of the node, and detect malicious nodes through the trust method.

Besides, for special DoS attacks, scholars have also proposed secure routing solutions. In view of the loopholes in the active routing protocol of optimized link state routing (OLSR), the author of [13] proposed an enhanced OLSR (EOLSR) protocol based on the trust mechanism to resist specific types of denial of service (DOS) attacks in the OLSR protocol -- node isolation attack.

4.3. Secure Routing Protocols against Black Hole Attacks

Scholars have studied a variety of secure routes to resist black hole attacks which is one of the common types of attacks. In the widely accepted dynamic source routing (DSR) of the on-demand routing protocol for mobile ad hoc networks, the discovery process of optimized routing and RREP packets can resist black hole attacks. The author of [14] proposed adding a validity value to the RREP packet in the
The DSR protocol to ensure no black hole attack along the road. The literature [15] proposed a scheme to verify the authenticity of the route by verifying the packet in DSR protocol to resist the Black hole attack. In the classic reactive routing protocol AODV, recognizing malicious routes and malicious nodes can also resist black hole attacks. The literature [16] proposes to identify malicious node with help of create black list and route addresses to against the black hole attacks in the AODV protocol. The literature [17] minimizes the black hole attack in the AODV protocol by checking whether the sequence number in the packet is the same as the destination sequence number. The author of [18] introduced a secure AODV routing protocol in which the destination node judges the validity of the RREQ reply path based on the threshold to resist black hole attacks.

4.4. Secure Routing Protocols against Gray Hole and Worm Hole Attacks
Currently, there are few routing protocols designed for gray hole attacks and wormhole attacks. The literature [12] found nodes with abnormal data packet transmission rates through virtual data packet calculation nodes and thresholds to select the corresponding secure routes. Because nodes with abnormal data packet transmission rates may actually intend to launch black hole attack, gray hole attack or wormhole attack, so this method can resist different types of attacks.

4.5. Secure Routing Protocols against Selfish Node Attacks
Selfish node detection is one of the ways to defend against selfish node attacks in multi-hop D2D networks. The literature [20] proposed a game theory scheme based on the AODV protocol based on packet forwarding rate (PFR) and routing density factor (RDF), which can detect selfish nodes and prevent malicious nodes in the system from transmitting data packets. And through the benefit matrix the author of [20] proved that only nodes that are cooperative in nature can benefit, thereby removing selfish nodes from the network.

Evaluating the trustworthiness or trust value of a node is another way to resist attacks from selfish nodes. Literature [21] proposed TEAB, a method for evaluating the trustworthiness of node behavior based on an adaptive time window, so that each node can choose a safe path consisting of only cooperative nodes. The literature [22] proposed a four-stage e-ARAN scheme based on OCEAN to detect and process authenticated selfish nodes. The literature [23] proposed a modular and configurable trust and reputation-based system MonConTR for secure routing to defend against selfish nodes in the network. MonConTR has 11 core components, and each of components implements different functions that can weigh security and performance.

Optimizing the path allocation of nodes in the network can also reduce selfish nodes. The literature [24] proposed a route based on simulated annealing to dynamically generate paths to optimize network load distribution to reduce selfish nodes in MANET networks.

4.6. Secure Routing Protocols against Malware Attacks
Different from other types of attacks, malware attacks will not only cause the interruption or paralysis of normal communication, but also cause the leakage of user information, thereby threatening the user’s property and privacy.

In the multi-hop D2D communication network, due to the lack of security measures provided by the network infrastructure, the threats posed by the malware will be more serious. Secure routing is one of the solutions to the problem of malware attacks in multi-hop D2D communication networks. However, so far, there have been few researches on secure routing for malware attacks in wireless distributed networks.

Game theory can be used to build models of attacker and defender to quantify the benefits of different routes to optimize route selection to resist malware attacks. The literature [25] proposed the iRouting based on the Malware Detection Game (MDG) in response to the problem that the MEC server may
launch malware attacks into the D2D network. The literature [26] proposed the Cluster-head Centered Fast Secure Routing (CCFSR) based on the Secure Routing Game (SRCG) to gainst the malware attackers inside the D2D network.

The literature [25] and literature [26] assume that each node in the D2D network is equipped with one or several anti-malware controls. As shown in Figure 2, the literature [25] abstracts the attacking entity that attempts to inject malware into the D2D network from the MEC server as the attacker, and abstracts the D2D network as the defender. As shown in Figure 3, the literature [26] abstracts malicious nodes with malware in the network as attackers, and abstracts the D2D network as defenders. The defender selects a secure route based on the malware detection capability and cost of each route, while the attacker selects different types of malware based on the benefits.

![Figure 2. The offensive and defensive model in the literature [25].](image)

![Figure 3. The offensive and defensive model in the literature [26].](image)

5. Conclusion
We can know from the literature [11-24] that the current research on secure routings in multi-hop D2D networks or ad hoc network is mainly based on evaluating the trustworthiness of the nodes, malicious node detection, and transmission path detection or optimization. The algorithms used in the research on secure routing include hash algorithms, game theory, simulated annealing, etc. Most research on secure routings is limited to specific types of attacks, such as black hole attacks, malware attacks, etc.

Researchers believe that the data packet forwarding rate of nodes that intend to launch DoS attacks, black hole attacks, or gray hole attacks may be quite different from normal nodes. The literature [22] proposed to send fake data packets from the source node to calculate the packet transfer rate and estimate the trust value of each node to resist DoS attacks, black hole attacks or gray hole attacks at the same
time. The literature [23] established a node trust mechanism that can resist attacks including selfish nodes and black hole attacks. The literature [27] finds abnormal nodes through traffic detection. In other words, the traffic detection and trust model can determine whether a node has malicious behaviors, such as selfish node attacks, black hole attacks, or gray hole attacks, so as to resist a variety of different attacks.

Nevertheless, for certain types of attacks, traffic detection still has its limitations, such as malware attacks. The literature [25,26] proposed the secure routings designed for malware attacks which essentially use anti-malware controls to complete malware detection and use certain decisions to optimize the routing process.

Consequently, in future research, how to ensure the security of the multi-hop D2D communication networks with the threat of multiple types attacks is still a problem worthy of research. One of the solutions may be combining different security mechanisms. But adding security mechanisms to the network is bound to affect the actual operating efficiency of the network or consume node energy within a certain range. So, it is important to balance safety and service.

In addition, the integration of new technologies including MEC and D2D can provide users in 5G networks with low-latency and high-reliability services. However, whether the new technology can help improve the security of D2D networks remains to be discussed. For example, literature [25] believes that the MEC server can be the malware attacker, while literature [26] believes that the MEC server can use the security resources to ensure that the cluster head itself does not launch malware attacks. Therefore, new technologies have brought both of opportunities and challenges to the security of D2D communication networks.

References

[1] Zhang P, Zhang T Y, and Zhang Y 2016 Survey of several key technologies for 5G J. Commun. 18(7) 15-29
[2] Qian Z H and Wang X 2016 Reviews of D2D technology for 5G communication networks J. Commun. 37(7) 1-14
[3] Haus M, Waqas M, Ding A Y, Li Y, Tarkoma S and Ott J 2017 Security and Privacy in Device-to-Device (D2D) Communication: A Review IEEE Commun. Surv. Tutor. 19(2) 1054-79
[4] Patil P, Marathe N and Jethani V 2016 Preventing DOS & MITM Attacks in “anonymous location based efficient routing protocol” in MANET 2016 Proc. IEEE. Conf.on Engineering and Technology (Coimbatore) (Washington: American/American IEEE Computer Society) pp 16-20
[5] Suarez-Tangil G, Tapiador J E, Peris-Lopez P and Ribagorda A 2014 Evolution, detection and nalysis of malware for smart devices IEEE Commun. Surv. Tutor. 16 2
[6] Papaleo G, Cambiasi E, Patti L and Aiello M Malware Development on Mobile Environments 2016 Proc. IEEE. 4nd. Int. Conf.on Future Internet of Things and Cloud Workshops (Vienna) (Washington: American/American IEEE Computer Society) pp 270-5
[7] Liu H, Xia M J and Wang Q T 2016 Research on a secure and energy-efficient routing protocol for Ad Hoc networks J Northeast Normal Uni(Nat Sci) 48(2) 83-8
[8] Venkatesan T P, Rajakumar P and Pitchaiikkannu A 2014 Overview of Proactive Routing Protocols in MANET 2014 Proc. 4nd. Int. Conf.on Communication Systems and Network Technologies (Bhopal) (Washington: American/American IEEE Computer Society) pp 173-7
[9] Istikmal, Adi K and Hendrawan 2017 Selective route based on snr with cross-layer scheme in wireless ad hoc network J Commun Netw-S Kor pp 1-13
[10] Tata C and Kadoch M 2015 Secure multipath routing algorithm for device-to-device communications for public safety over LTE heterogeneous networks 2015 Proc. 3rd. Int. Conf.on Future Internet of Things and Cloud (Keynote) (Washington: American/American IEEE Computer Society) pp 212-7
[11] Patil P, Marathe N and Jethani V 2016 Improved ALERT protocol in MANET with strategies to prevent DOS & MITM attacks 2016 Int. Conf.on Automatic Control and Dynamic Optimization Techniques (Pune) (Washington: American/American IEEE Computer Society) pp 372-7
[12] Kumar J A and Choorasiya 2017 A Security enhancement of AODV routing protocol in mobile ad hoc network 2017 Proc. 2nd. Int. Conf.on Communication and Electronics Systems (Coimbatore) (Washington: American/American IEEE Computer Society) pp 958-64
[13] Marimuthu M and Krishnamurthi L 2013 Enhanced OLSR for defense against DOS attack in ad hoc networks J Commun Netw-S Kor 15 1 pp 31-7
[14] Deshmukh S R and Chatur N 2016 Secure routing to avoid black hole affected routes in MANET 2016 Proc. Symp.on Colossal Data Analysis and Networking (Washington: American/American IEEE Computer Society) pp 1-4
[15] Bhardwaj A 2014 Secure routing in DSR to mitigate black hole attack 2014 Proc. Int. Conf.on Control, Instrumentation, Communication and Computational Technologies (Kanyakumari) (Washington: American/American IEEE Computer Society) pp 985-9
[16] Singh K and Sharma S 2017 A new technique for AODV based secure routing with detection blackhole in MANET 2017 Proc. IEEE. Int. Conf.on. Power, Control, Signals and Instrumentation Engineering (Chennai) (Washington: American/American IEEE Computer Society) pp 1528-34
[17] Chengetanai G 2018 Minimising Black Hole Attacks to Enhance Security in Wireless Mobile Ad Hoc Networks Proc. IST-Africa Week Conf. (Gaborone) (Washington: American/American IEEE Computer Society) pp 1-7
[18] Yadav S, Trivedi M C, Singh V K and Kolhe M L 2017 Securing AODV routing protocol against black hole attack in MANET using outlier detection scheme Proc. IEEE. 4th. Uttar Pradesh Section Int. Conf.on Electrical, Computer and Electronics (Mathura) (Washington: American/American IEEE Computer Society) pp 1-4
[19] Elmahdi E, Yoo S and Sharshembiev K 2018 Securing data forwarding against blackhole attacks in mobile ad hoc networks Proc. IEEE. 8th. Annual Computing and Communication Workshop and Conf. (Las Vegas) (Washington: American/American IEEE Computer Society) pp 463-7
[20] Das D, Majumder K and Dasgupta A 2016 A game-theory based secure routing mechanism in mobile ad hoc network 2016 Proc. Int. Conf.on Computing, Communication and Automation (Noida)(Washington: American/American IEEE Computer Society) pp 437-42
[21] Umeda S, Takeda S and Shigeno H 2015 Trust evaluation method adapted to node behavior for secure routing in mobile ad hoc networks Proc. Eighth Int. Conf.on Mobile Computing and Ubiquitous Networking (Hakodate) (Washington: American/American IEEE Computer Society) pp 143-8
[22] Jangra A, Shalini and Goel N 2012 e-ARAN: Enhanced Authenticated Routing for ad hoc networks to handle selfish nodes Proc. IEEE. Int. Conf. on Advances In Engineering, Science And Management (Nagapattinam) pp 144-9
[23] Hatzivasilis G, Papaefstathiou I and Manifavas C 2014 ModConTR: A modular and configurable trust and reputation-based system for secure routing in ad-hoc networks Proc. IEEE/ACS.11th. Int. Conf.on Computer Systems and Applications (Doha) (Washington: American/American IEEE Computer Society) pp 56-63
[24] Prabaharan S B, Ponnusamy R 2016 Secure and energy efficient MANET routing incorporating trust values using hybrid ACO Proc. Int. Conf. on Computer Communication and Informatics (Coimbatore) (Washington: American/American IEEE Computer Society) pp 1-8
[25] Panaoussis E, Karapistoli E, Elsemary H, Alpcan T, Khuzani M, and Economides A A 2017 Game theoretic path selection to support security in device-to-device communications Ad Hoc Netw 56 28-42
[26] Lv Y, Feng W, Xiao A and Bao X 2020 Cluster-head Centered Fast Secure Routing based on Game theory for Device-to-Device Communication Wireless Pers Commun 113(4) 2079- 106
[27] Saurabh V K, Sharma R, Itare R and Singh U 2017 Cluster-based technique for detection and prevention of black-hole attack in MANETs Proc. Int. Conf. on Electronics, Communication and Aerospace Technology (Coimbatore) (Washington: American/American IEEE Computer Society) pp 489-94