International Journal of Scientific Research & Engineering Trends
Volume 9, Issue 5, Sept-Oct-2023, ISSN (Online): 2395-566X

A Survey of the Self-Operative Trust Scheme against MANET Disruptions

Assistant Professor Sujeet Gautam
Dept. of Computer Science Engg.
Madhyanchal Professional University

Abstract- A mobile ad hoc network is a group of nodes that lacks an infrastructure, making it simple to set up and deploy right away. All nodes in this type of network perform the role of routers in addition to their normal operations. All nodes are allowed to move at random in a MANET because of the network's mobility and dynamic nature, which causes frequent changes in topology. The complexity of routing the packets from source to destination is therefore invited. The numerous difficulties and problems relating to the trust value or scheme in the mobile ad hoc network are discussed in this article, and we also offer the survey for the network's trust scheme.

Keywords- Mobile Ad-hoc Networks, Attack, Quality of Service, Evolutionary Self-Cooperative Trust, Dynamic Source Routing.

I. INTRODUCTION

MANETs are mobile ad hoc networks. These networks are made up of a collection of wireless mobile nodes that dynamically exchange data among one another without the need for a fixed base station or any centralized administration. MANETs may be quickly constructed in a wide range of dissimilar settings, such as search and rescue, emergency operations, and wartime communications, thanks to their self-organizing nature. However, the adaptability and self-organizing features of MANETs cause the change of topology in an unpredictable way. Most of the time, each mobile node with limited transmission range has to seek assistance of its neighboring nodes for data transmissions. As a result, the performance of MANETs largely depends on the reliable routing among nodes.

Computer networks were originally developed to operate by connecting computers together with wires and transmitting data over these wires. Network sizes and occurrences increased creating a requirement for inter-network communication. This led to the development of the Internet and its suite of protocols. The use of the Internet and its applications became ubiquitous. A need for providing network access to entities while not physically attached to the wired network arose. To enable this wireless networking was developed, providing devices with methods to connect to a wired network using radio wave technologies through wireless access points. Simultaneously, telephone networks were undergoing a similar transformation [3].

A collection of autonomous, dynamic, wireless, and mobile nodes that may be set up without the aid of any pre-existing infrastructure is known as a mobile ad hoc network (MANET).. As every node in a MANET is a wireless node, it has

Limited transmission range, making it impossible to directly converse with every node in the network. Due to this, MANET is now a multihop network. Every node in a MANET randomly enters and exits it, causing the topology of this network to alter over time. This characteristic of MANETs causes the mobile nodes' locations to vary frequently, which complicates the routing process. The nodes' transmission power is constrained because they are mobile and cannot receive a constant power supply [4].

Efficient routing protocols are required because MANETs are employed in highly dynamic situations, enabling communication between the nodes. Depending on the protocol's primary objective, several routing metrics may be employed. It is suggested to use a protocol that combines connection state with geographic routing. For small distances, link-state routing is employed, whereas geo-forwarding is used for large distances. The outcomes demonstrate the proposal's great scalability for a growing number of nodes. The shortest path metric is typically used for routing in MANETs, although several proposals additionally considered metrics to reduce interference or were based on multi-objective reduction that included the connection duration probability [2].

In MANETs, Quality of Service (QoS) routing is a crucial task. QoS routing must assure end-to-end quality in addition to determining the routes from a source to a destination, typically in terms of bandwidth or delay [4]. MANET nodes can only connect with each other when they are physically within communication range of one another, therefore developing a safe and effective routing protocol that can also guarantee overall quality of service

during the routing process is a significant task. The dynamic nature of MANETs makes it challenging to guarantee QoS when the receiver is far from the transmitter, i.e., the destination is outside of the transmission range of the transmitter. Dynamic quality changes can result in occasional link failures and force nodes to connect to other nodes [5].

Routing disruption attackers can secretly choose any aforementioned attack pattern and cause significant packet loss. In the below figure we observe that the packet delivery ratio reduces more than 30 percent with the presence of 4 percent disruption attackers among the nodes. Furthermore, the adverse effect of attacks will exacerbate when the node speed increases. Notice that the faster malicious nodes move, the larger region they can cover. Due to MANETs' open design, it is rather typical for rogue nodes to hide within the network and delete packets in an effort to conserve energy or disrupt network operations. The next sections of this essay are structured as follows. In the first section, we give an overview of the wireless sensor network and attack. The reactive routing protocol is covered in Section II. The associated work for the trust scheme in mobile ad hoc networks is covered in Section III, and the conclusion and discussions of the future scope is provided in Section

II. ROUTING PROTOCOL FOR REACTIVE

Dynamic Source Routing, one of the main on-demand routing protocols, reduced the bandwidth used by control packets by removing periodic database update messages. QoS Guided Route Discovery and Securing Quality of Service Route Discovery are two examples of secure protocols based on DSR. A node may indicate the desired QoS metrics in the QoS guided discovery of routes protocol; these metrics must be offered by the chosen path. Although it used bandwidth, latency, and jitter as measurements, it had trouble figuring out what resources were available at a certain node. A safe on demand routing protocol is the quality of service route discovery protocol. which applies symmetric encryption.

The computation of the route takes bandwidth and delay into account, but does not adequately account for the capacity of the intermediate node in terms of node power, memory, and storage. Ariadne is a reliable on-demand protocol that is based on TESLA, a successful broadcasting system. Ariadne lacks a feedback system and is unaware of any assaults on the route that has been found. Nodes are divided into selfish and unselfish nodes in CONFIDANT (Cooperation of Nodes Fairness in Dynamic Ad-hoc Network), which employs global reputation values. By detecting routing misbehavior, it takes care of optimal forwarding and traffic redirection [6]. A destination Sequence Number is used by the popular on-demand routing protocol AODV to create pathways to the destination node. Utilizing resources smoothly is not.The utilization of resources is not optimal and also there is no provision of security in AODV the best and that AODV does not offer any security.

III. RELATED WORK

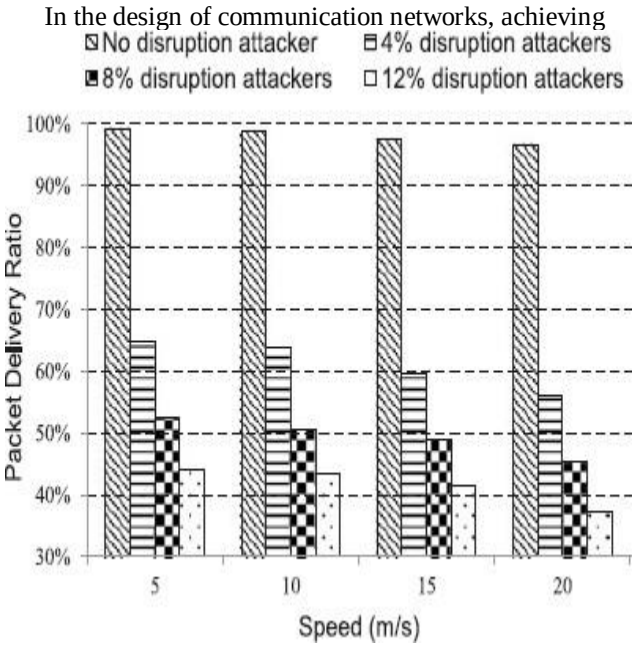

Figure 1: The effect of disruption attackers with varying speeds.

reliable routing has always been a challenge. Mobile ad hoc networks (MANETs) have the most hostile networking environment due to the lack of fixed infrastructure, the open nature of their transmission media, and their dynamic network topology. Additionally, these qualities make the Routing protocol design in MANETs becomes significantly more difficult. [1] The authors of this work suggest an evolutionary self-cooperative trust (ESCT) system that mimics human cognitive function and relies on trust-level information to defend against a variety of routing disruption assaults.

In this system, mobile nodes will communicate trust information and use their own cognitive judgment to examine received trust information. Each node eventually changes its cognition dynamically to block harmful creatures. The most alluring aspect of ESCT is that even if internal attackers are aware of how the security mechanism operates, they cannot compromise the system. across this study, we assess the effectiveness of the ESCT scheme across a range of routing disruption attack scenarios. The simulation results support ESCT. method encourages network scalability and guarantees routing efficacy in MANETs in the presence of attackers who attempt to interrupt routing.

[2] Because the nodes that do not behave properly are excluded from the routes, communication between the nodes is not disturbed if certain MANET nodes maliciously drop packets that must be forwarded, and the message will reach its destination. The proposal adds new packets to the protocol, increasing protocol energy usage. The biggest difference in consumption is caused by the usage of promiscuous mode to identify rogue nodes. As a result, a node receives and analyzes all data transferred within its wireless range, which requires more energy.

[3] Author explains in this paper As dynamic feedback mechanisms are added to an ad hoc network to control node misbehavior, the CONFIDANT (Cooperation Of Nodes: Fairness In Dynamic Ad-hoc Network) on DSR (Dynamic Source Routing Protocol) is simulated to assess how the network performance changes. A significant amount of simulations have been run to assess the effectiveness of CONFIDANT reinforced DSR. According to the simulation data, CONFIDANT dramatically lowers the evil throughput and bad drop rate by up to more than 50%. It proves that CONFIDANT can effectively.

[5] In this paper author propose a trust-based secure QoS routing scheme by combining social and QoS trust. The primary approach of the proposed scheme relies on mitigating nodes that exhibit various packet forwarding misbehavior and on discovering the path that ensures reliable communication through the trust mechanism. The scheme would select the best forwarding node based on packet forwarding behavior as well as capability in terms of QoS parameters, such as residual energy, channel quality, link quality, etc.

They will present an adversary model for packet dropping attack against which we evaluate the proposed scheme. [6] This paper proposed a Trust Based Routing Scheme called Trust Based AODV (TAODV), in which a trust metric is assigned to the nodes based on the behaviour of the nodes. An abnormal behavior initiated a route rediscovery and therefore such an optimal scheme is found to have significant improvement in various QoS metrics when compared to the existing scheme. The performance of TAODV has been ,assuming there is no loss of packets due to insufficient energy of the nodes. Future work would be to analyze the performance of the network when the nodes have insufficient energy to forward the packets.

[7] In this paper author design a decentralized trust management scheme (DTMS) to filter out malicious nodes in DTNs. First, the number of forwarding evidence are combined with the energy consumption rate of the nodes to formulate direct trust. Then, a recommendation trust is computed from the indirect trust, recommendation credibility and recommendation familiarity. Recommendation credibility and familiarity improve the overall recommendation trust by filtering out dishonest recommendations. A comparative analysis of DTMS is performed against a Cooperative Watchdog Scheme (CWS), Recommendation Based Trust Model (RBTM) and Spray & Wait protocol. The results show that DTMS can effectively deal with malicious behaviors in DTNs including trust related attacks. [8] In this article, they focus on wireless technologies and potential challenges to provide a communication's vehicle-to-vehicle (V2V) or vehicle-to-X(V2X). In particular, we discuss the challenges and review the state-of-the-art wireless

Solutions for internet of vehicle (IOV). Connected cars themselves as new born of new technologies, are the next frontiers for the automobile revolution and the key to thee volution towards the next generation of intelligent transport systems that enable information sharing and communication between vehicles and their internal and external environment. Moreover, connected cars are the main use cases of internet of things (IOT), yet they are the least understood in terms of cyber security. They also identify future research issues for building connected vehicles and solutions which have been proposed by several researchers.

[9] The proposed work provides man-in-the-middle attack resistance and mutual authentication using certified public key and out-of-band sense-able attributes. As the CA pre-processes every vehicles public key and unchangeable attributes, there is no way that man-in-the-middle can fake the public key or the unchangeable attributes. Also, the out- of-band attributes are sense-able and can be confirmed, while moving on the road. There is no need to communicate with the CA during the real- time session key establishment of a secret key based on the mutual authentication of vehicles. The proposed approach is simple, efficient and ready to be employed in current and future vehicular networks. [10] In this paper, they propose an intelligent naïve Bayesian probabilistic estimation practice for traffic flow to form a stable clustering in VANET, briefly named ANTSC.

The proposed scheme aims to improve routing by employing awareness of the current traffic flow as well as considering the blend of several factors, such as speed difference, direction, connectivity level, and node distance from its neighbors by using the intelligent technique. The proposed technique has proven to be more strong, stable, robust, and scalable than existing ones. [12] In this paper, they perform sensitivity analysis of TRS-PD which is carried out by varying values of different parameters in distinct network scenarios in the existence of three distinct packet dropping attacks. In addition, this work summarizes the attack-pattern discovery mechanism, trust model, and routing mechanism adopted by TRS-PD in order to counter the adversaries which follow certain attack patterns along with other

adversaries. Experiments conducted with network simulator-2 indicate the correct choices of parameter values for distinct network scenarios.

IV. CONCLUSIONS AND FUTURE SCOPE

Mobile ad-hoc networks (MANETs) are pervasive autonomous networks that will play a vital role in future Industrial Internet-of-Things communication, where smart devices will be connected in a completely distributed manner. However, due to lack of infrastructure and absence of centralized administration, MANETs are shrouded with various security threats. Some internal mobile nodes in these resource constrained networks may compromise the routing mechanism in order to launch denial-of-service attacks to carry out distinct kinds of packet forwarding misbehaviors. Here we resent the survey for the trust scheme in mobile ad-hoc network, also gives the directions for future work to improve the quality of services and enhance the performance of mobile ad-hoc network by using trust scheme or values.

REFERENCES

[1] Ruo Jun Cai, Xue Jun Li , Peter Han Joo Chong, "An Evolutionary Self-Cooperative Trust Scheme Against Routing Disruptions in MANETs", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 18, NO. 1, JANUARY 2019, pp 42-57.

[2] Andrea Lupia, Floriano De Rango, "Evaluation of the Energy Consumption Introduced by a Trust - Management Scheme on Mobile Ad-hoc Networks", Journal of Networks, 2015, pp1 -113.

[3] Yumana Zaidi, Naveen Kumar, Parul Saharavat, " Designing of Authentication Based Security in MANETs", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2018, pp 61-65.

[4] Swetha M S, Dr. Thungamani M, Ankita Mishra, "Enhancement of Performance Analysis in Anonymity MANET through Trust-Aware Routing Protocol", International Journal of Advance Research in Computer Science and Management Studies, 2017. Pp 104-110.

[5] Muhammad Salman Pathan, Nafei Zhu, Jingsha He, Zulfiqar Ali Zardari, Muhammad Qasim Memon, Muhammad Iftikhar Hussain, "An Efficient Trust-Based Scheme for Secure and Quality of Service Routing in MANETs", MDPI 2018, pp 1-16.

[6] D. Sylvia, Jeevaa Katiravan, D. Srinivasa Rao, "Trust based Routing in Wireless Ad Hoc Networks under Adverse Environment", International Journal of Computer Applications 2016, pp 23-28.

[7] Philip Asuquo, Haitham Cruickshank, Chibueze P. Anyigor Ogah, Ao Lei, and Zhili Sun, "A Distributed Trust Management Scheme for Data Forwarding in Satellite DTN Emergency Communications", 2016, pp 1-12.

[8] S. Tbatou , A.Ramrami , Y. Tabii , "Security of communications in connected cars Modeling and safety assessment", Conference Paper , March 2017, pp 1-8.

[9] Shlomi Dolev, Lukasz Krzywiecki, Nisha Panwar, Michael Segal, "Certificating Vehicle Public Key with Vehicle Attributes", SAFECOMP 2013, 32nd International Conference on Computer Safety, Reliability and Security, Sep 2013, pp 1-18.

[10] AMJAD MEHMOOD, AKBAR KHANAN, ABDUL HAKIM H. M. MOHAMED, SAEED MAHFOOZ, HOUBING SONG, SALWANI ABDULLAH, "ANTSC: An Intelligent Naïve Bayesian Probabilistic Estimation Practice for Traffic Flow to Form Stable Clustering in VANET", IEEE Volume-6, 2018. Pp 4452-4461.

[11] Sachin P. Godse, Parikshit N. Mahalle, Sanjeev J. Wagh, " Rising Issues in VANET Communication and Security: A State of Art Survey", International Journal of Advanced Computer Science and Applications, 2017, pp 245- 52.

[12] RUTVIJ H. JHAVERI, NARENDRA M. PATEL, YUBIN ZHONG, AND ARUN KUMAR SANGAIAH, "Sensitivity Analysis of an Attack-Pattern Discovery Based Trusted Routing Scheme for Mobile Ad-Hoc Networks in Industrial IoT", IEEE Access 2018, pp 20085-20103. etc. His areas of Interests are Antenna & Wave Propagation, Digital Signal Processing, Wireless Communication, Image Proces