ISSN: 2581-3404 (Online)
International Journal of Innovative Research in Technology and Management (IJIRTM), Volume-3, Issue-3, 2019

Self Co-Operative Trust Scheme against Disruptions in MANETs: A Survey

Priyanka Sharma[1], Prof. Jitendra Mishra[2]

[1]M. Tech Scholar, Department of EC, PCST, Bhopal (India)

[2]Head & Professor, Department of EC, PCST, Bhopal (India)

[1]priyankasharma02990@gmail.com, [2]jitendramishra@gmail.com

ABSTRACT

A Mobile ad Hoc Network is a collection of nodes which is an infrastructure less network and hence can be easily established and deployed instantly. In addition to their normal operation, all the nodes in this kind of network act as routers as well. Because of the mobility and dynamic nature of the network, all the nodes are free to move randomly and hence topology of a MANET changes very frequently. This invites the complexity of routing the packets from source to destination. In this paper we discuss about the various challenges and issues regarding the trust value or scheme in the mobile ad-hoc network and also present the survey for the trust scheme in network.

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

INTRODUCTION

Mobile ad-hoc networks (MANETs). These networks consist of a group of wireless mobile nodes that dynamically exchange data among themselves without the reliance on any centralized administration or fixed base station. Self-organizing characteristic enables MANETs to be easily established in a wide variety of disparate situations, such as rescue, emergency operations, and battlefield communications. However, mobility and self-organizing characteristics 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 mobile ad hoc network (MANET) is a communications network that can be defined as a collection of independent, dynamic, wireless and mobile nodes that can be established without the help of any pre-existing infrastructure. As every node in a MANET is a wireless node, it has a limited transmission range, and hence cannot communicate with all the other nodes in the network directly. This has lead MANET to be a multi hop network. Every node in a MANET moves randomly in and out of it and hence the topology of this network changes dynamically. This feature of MANETs also results in frequent changes in the location of the mobile nodes which makes routing task more complicated. As the nodes are mobile, and hence there is no continuous power supply, the transmission power of the nodes is limited [4].

MANETs are used in very dynamic environments, so scalable routing protocols are needed to allow the communication between the nodes. Various routing metrics could be used, depending on which is the main aim of the protocol. A protocol combining link state and geographical routing is proposed. The link-state routing is used for short distances, while for long distances the geo-forwarding is applied. The results show the high scalability of the proposal for increasing number of nodes. Usually the routing in MANETs follows the shortest path metric, but many proposals took into account metrics to reduce interference or based on multi-objective minimization using also the link duration probability [2].

Quality of Service (QoS) routing is a necessary function in MANETs. In addition to finding the routes from a source to a destination, QoS routing also needs to ensure end-to-end quality, usually in terms of bandwidth or delay [4]. A major challenge for MANETs is the design of a secure and efficient routing protocol that can also ensure the overall quality of service during the routing process as MANET nodes communicate with each other only when they are located within the communication range of each other. When the receiver is far away from the transmitter, i.e., the destination is out of the transmission range of the transmitter, the dynamic nature of MANETs makes it difficult to ensure QoS since the node-to-node channel and link quality changes dynamically which may result infrequent link failures and cause nodes to make connections with 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 the open nature of MANETs, it is rather common that some malicious nodes may hide in the network and drop the packets in order to save the energy or break the network operation.

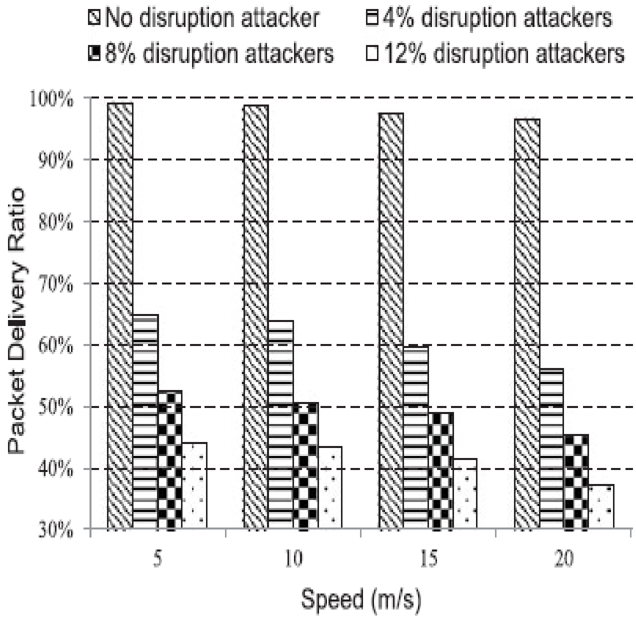

Figure 1: The effect of disruption attackers with varying speeds.

The rest of this paper is organized as follows in the first section we describe an introduction of about the wireless sensor network and attack. In section II we discuss about the reactive routing protocol, In section III we discuss about the related work for the trust scheme in mobile ad-hoc network, finally in section IV we conclude and discuss the future scope.

II REACTIVE ROUTING PROTOCOL

One of the major on demand routing protocol is Dynamic Source Routing, which eliminated the periodic table update messages and thereby conserved the bandwidth consumption by control packets. Some of the secure protocols based on DSR are QoS Guided Route Discovery, Securing Quality of Service Route Discovery. In QoS guided route discovery protocol, a node is allowed to specify the desired QoS metrics, which must be provided by the selected path. It uses bandwidth, latency and jitter as the metrics but had difficulty in determining the resources available at a particular node. Securing Quality of Service Route Discovery is a secure form of on demand routing protocol, which implements symmetric cryptography. It includes bandwidth and latency in the route computation process, but has not given due consideration to the capability of intermediate node in terms of node power, memory and storage. Ariadne is a secure on demand protocol, based on the efficient broadcasting scheme TESLA. Ariadne has no feedback mechanism and has no knowledge of attacks on the discovered route. CONFIDANT (Cooperation of nodes fairness in dynamic ad-hoc network): categories nodes into selfish and unselfish nodes and uses global reputation values. It takes care of optimal forwarding and traffic diversion, by identification of routing misbehavior [6]. AODV is a dominant on-demand routing protocol that uses a destination Sequence Number to establish paths to the destination node. The utilization of resources is not optimal and also there is no provision of security in AODV.

III RELATED WORK

How to achieve reliable routing has always been a major issue in the design of communication networks, among which mobile ad hoc networks (MANETs) possess the most adversarial networking environment due to the absence of fixed infrastructure, the nature of open transmission media and the dynamic network topology. These characteristics also make the design of routing protocols in MANETs become even more challenging.

[1] In this paper author propose an evolutionary self-cooperative trust (ESCT) scheme that imitates human cognitive process and relies on trust-level information to prevent various routing disruption attacks. In this scheme, mobile nodes will exchange trust information and analyze received trust information based on their own cognitive judgment. Eventually, each node dynamically evolves its cognition to exclude malicious entities. The most attractive feature of ESCT is that they cannot compromise the system even if the internal attackers know how the security mechanism works. In this paper, we evaluate the performance of ESCT scheme under various routing disruption attack situations. Simulation results affirm that ESCT scheme promotes network scalability and ensures the routing effectiveness in the presence of routing disruption attackers in MANETs. [2] The communication between the nodes is not disrupted if some nodes in the MANET drop maliciously packets that have to be forwarded, and the transmission will reach its destination, because the nodes that not behave correctly are excluded from the routes. The proposal introduces new packets in the protocol, therefore the energy consumption increases. The main difference in terms of consumption is due to the use of promiscuous mode to detect nodes behaving maliciously, so a node receives all the data transmitted in its wireless range, and consequently it consumes more energy to receive and analyze them. [3] In this paper author present The CONFIDANT (Cooperation Of Nodes: Fairness In Dynamic Ad-hoc Network) on DSR (Dynamic Source Routing Protocol) is simulated in order to evaluate how the network performance changes as dynamic feedback mechanisms are introduced in an ad hoc network to control the node misbehavior. A large amount of simulations have been conducted to evaluate the performance of CONFIDANT fortified DSR. The simulation results show that CONFIDANT significantly decreases the evil throughput and evil 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 behaviour 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 the evolution 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.

Priyanka Sharma received her Bachelor`s degree in Electronics & comunication, BIT, Bhopal, M.P., in 2011. Currently she is pursuing Master of Technology Degree in Electronics & Comunication (Digital communication) from PCST, (RGPV), Bhopal, Madhya Pradesh India. Her research area include Mobile Ad-hoc networks.

Mr. **Jitendra Mishra** he is Associate Professor and Head of the Department of Electronics and communication in PCST, Bhopal (RGPV). His received Master of Technology and Bachelor's of engineering respectively in Digital communication from BUIT, Bhopal and from RGPV, Bhopal. He has more than 11 years of teaching experience and publish 35+ papers in International journals, conferences etc. His areas of Interests are Antenna & Wave Propagation, Digital Signal Processing, Wireless Communication, Image Processing etc.