Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.754735

STUDY AND ANALYSIS OF TRUST BASED DATA SHARING MECHANISM FOR MOBILE AD HOC NETWORK (MANET)

[1]Dr. S. Sujiya, [2]Mr. L. Pradeep, [3]Mr. P. S. Prasanna.
[1]Assistant Professor, Department of Computer Applications, Dr. SNS Rajalakshmi College of Arts & Science, Coimbatore.
[2]PG Student, II MCA, Department of Computer Applications, Dr. SNS Rajalakshmi College of Arts & Science, Coimbatore.
[3]PG Student, II MCA, Department of Computer Applications, Dr. SNS Rajalakshmi College of Arts & Science, Coimbatore.

Abstract: - Mobile ad hoc networks (MANETs) are spontaneously deployed over a geographically limited area without well-established infrastructure. The networks work well only if the mobile nodes are trusty and behave cooperatively. Due to the openness in network topology and absence of a centralized administration in management, MANETs are very vulnerable to various attacks from malicious nodes. In order to reduce the hazards from such nodes and enhance the security of network, this paper presents a dynamic trust prediction model to evaluate the trustworthiness of nodes, which is based on the nodes' historical behaviors, as well as the future behaviors via extended fuzzy logic rules prediction. The primary approach of the proposed scheme relies on mitigating nodes that exhibit various packets 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. We will present an adversary model for packet dropping attack against which we evaluate the proposed scheme.

Keywords: - MANET, Routing Protocols, Security, Trust Node, Data Sharing, Aggregation, Estimation.

1. INTRODUCTION

Wireless networks allow a more flexible model of communication than traditional networks since the nodes is not limited to a fixed physical location. Unlike cellular wireless networks, mobile ad hoc networks (MANETs) are spontaneously deployed over a geographically limited area without well-established infrastructure. They are widely deployed in applications such as the disaster recovery and distributed collaborative computing, where routes are multi-hop and inter-agent communication are achieved by message transmission. Each node acts as a wireless router which delivers packets for neighbors to reach the intended destination, which allows MANETs to accommodate high mobility and frequent topology changes. Meanwhile, a MANAT works well only if the mobile nodes are trusty and behave cooperatively [1].

The proliferation of mobile devices has led to the growth of 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. There are three types of routing disruption attacks that can be easily launched in MANETs:

1) Active Black Hole Attack,
2) Passive Black Hole Attack and
3) Gray-Hole Attack.

In active black hole attacks, the attackers always claim that they have the shortest path to the destination even if they do not have any proper routing information. Active black hole attackers can attract considerable amount of data packets and drop them silently.

In passive black hole attacks, attackers help forwarding routing messages but discard all passing-by data packets. In gray-hole attacks, instead of dropping all passing-by data packets,

Gray-hole attackers may selectively forward those data packets that can maximize their own interests. Routing disruption attackers can secretly choose any aforementioned attack pattern and cause significant packet loss. 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. An evolutionary self-cooperative trust (ESCT) scheme that imitates human cognitive process and relies on trust-level information to prevent various routing disruption attacks [2]. 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 primary security threat to MANETs routing is the possibility of an adversary disrupting traffic by compromising the routing mechanisms. The distribution of false routing information allows the potential of unintended network routing loops, denial of service attacks, or other nonfunctional routes. These attacks may hinder or prohibit the communication vital to fulfilling the mission of networked nodes [3]. It is therefore critical for nodes to dynamically determine the validity of routing information prior to making routing decisions. With authentication and encryption mechanisms, secure routing protocols have been developed to ensure properties such as confidentiality and integrity. These protocols require a centralized trusted third party, which is impractical for MANETs [4]. Moreover, the traditional cryptosystem based security mechanism is typically used to resist the external attacks. They show inefficiency in handling the attacks from the internal malicious nodes which may lead to serious influence on the security, the confidentiality, and the life cycle of the whole network. Recently a new class of routing protocols in MANETs has been proposed, called trusted routing protocols. The trust-based routing protocols are not absolutely secure, but certainly have an accurate measure of reliability in them. Careful selection of a dependable trusted route may mitigate the impairment from malicious nodes, however, it is also critical to route packets to destinations without generating excessive overhead [5]. Therefore, how to design an efficient and effective trusted routing protocol is a major challenging issue for this network.

The paper is organized in following sections: section 2 describes the related work on statement of the problem, section 3 describes the existing methodology and its drawbacks,

section 4 about the proposed work and its modules, and section 5 conclude the proposed work and future studies.

2. LITERATURE REVIEW

Secure routing plays an important role in reliable network performance. Conventional secure routing protocols [11] employ a variety of cryptographic tools to prevent active attackers from injecting false information into a network. As a harmful and easy-to-implement type of attack, a malicious node simply replays all the outgoing routing packets from a valid node to forge the latter node's identity; the malicious node then uses this forged identity to participate in the network routing, thus disrupting the network traffic. Those routing packets, including their original headers, are replayed without any modification.

Awan, K. A., et al., (2021), proposed mechanism is a multi-leveled centralized approach utilizing both the infrastructure and vehicles to sustain a secure environment [6]. VANET is a heterogeneous network, due to which the VANET environment exposes to have various security and privacy challenges. In the future, the automobile industry will progress towards assembling electric vehicles containing energy storage batteries employing these resources to travel as an alternative to gasoline/petroleum. These vehicles may have the capability to share their energy resources upon the request of vehicles having limited energy resources. The proposed vTrust can aggregate and propagate the degree of trust to enhance scalability. The node that requests to obtain the energy resources may have to maintain a specified level of trust threshold for earning resources. The proposed mechanism can efficiently manage a secure environment during resource sharing by maintaining average malicious nodes detection of 91.3% and average successful energy sharing rate of 89.5%, which is significantly higher in comparison to the existing approaches.

Alnumay, W., et al., (2015), finds the solution for trust model for an IoT-MANET [7]. The proposed trust model combines both direct and indirect trust opinion in order to calculate the final trust value for a node. A Beta probabilistic distribution is used to combine different trust evidences and direct trust has been calculated. The theory of ARMA/GARCH has been used to combine the recommendation trust evidences and predict the resultant trust value of each node in multi-step ahead. Further, a routing protocol has been designed to ensure the secure and reliable end-to-end delivery of packets by only considering trustworthy nodes in the path. Simulation results show that our proposed trust model outperforms similar existing trust models.

Kumar, S., & Dutta, K. (2018), introduced a dynamic trust based intrusion detection technique is presented to detect and isolate the selfish nodes from the network, where the direct trust degree based on direct communication interactions and indirect (recommended) trust degree based on the neighbors' recommendations are taking into account to accurately judge the selfishness nature of the nodes [8]. The proposed mechanism addressed that, there are some nodes that may intentionally turn themselves to behave selfishly in order to conserve their valuable resources. The selfish behaviour of such nodes drastically reduces the desired degree of cooperation amongst the mobile nodes. Over the course of time, the non-cooperative activities of, such selfish nodes would paralyze the normal functioning of the whole network. Therefore, these types of nodes should be detected and isolated from the network, as soon as they begin to exhibit their selfish behaviour. The results obtained throughout the simulation

experiments clearly show the feasibility and effectiveness of the proposed intrusion detection technique.

Vatambeti, R. (2020), proposed a novel Grey Wolf Trust Accumulation (GWTA) Schema in wireless mesh network architecture, thus the attacks are identified by the finest function of the GWTA model [9]. Moreover, the predicted attacked nodes are replaced to the last position of the network medium to prevent the packet loss. security is one of the key concerns in routing because of the moving nodes; thus it is usually affected by Black Hole and Grey Hole attack. These types of malicious activities are more harmful to the network channel, and once the attack is happened it is difficult to predict and mitigate. Furthermore, the comparison studies proved the effectiveness of the proposed model by attaining less packet drop and high throughput ratio rate.

Ambekar, R. K., & Kolekar, U. D. (2022) finds the security factor of each node in the MANET, and the neighbor nodes are selected based on the defined security factor [10]. The proposed routing method has four models for defining the security factor, namely the trusted model, energy model, delay model, and the mobility model. The proposed multipath routing determines the secured route between the sender and receiver based on the selected neighbor nodes. Finally, data communication is performed through the selected multipath. The performance of the proposed multipath routing is analyzed with the existing methods, such as topology-hiding multipath routing protocol, Fractional lion optimization to topology-hiding multi-path routing, and Adaptive Fractional lion optimization to topology-hiding multi-path routing for the performance metrics, such as throughput, delay, energy, and packet drop rate (PDR). Simulation results show that the proposed multipath routing has the better performance.

3. EXISTING METHODOLOGY

Trust management in MANETs is needed when participating nodes, without any previous interactions, desire to establish a network with an acceptable level of trust relationships among themselves. Trust management, including trust establishment, trust update, and trust revocation, in MANETs is also much more challenging than in traditional centralized environments [12]. For example, collecting trust information or evidence to evaluate trustworthiness is difficult due to changes in topology induced by node mobility or node failure. Further, resource constraints often confine the trust evaluation process only to local information. The dynamic nature and characteristics of MANETs result in uncertainty and incompleteness of the trust evidence, which is continuously changing over time [13].

An evolutionary self-cooperative trust (ESCT) scheme that can be regarded as a value-added security mechanism on top of conventional routing protocols. As the name indicates, this scheme is based on two pillars:

1. On the one hand, every node executes self-detection to evaluate the trust levels of other nodes (benign or malicious) independently.
2. On the other hand, they share self-detection results with their direct neighbors to help peers to perform cooperative detection to get further trust information about the network.

Each node puts more confidence in those trust information (properties of peers) that are explored through self-detection. Furthermore, self-detection experience will influence the attitude of a node (optimistic or pessimistic) towards the network, and consequently affect its

decision upon receiving shared trust information from neighbors [14]. Drawbacks of Existing System

- Energy Consumption: Overhearing technique is a fundamental building block in many trust based routing systems. One of the major drawbacks of this technique is that it consumes much more energy than ESCT, because each node has to keep monitoring its neighbors.
- Internal Attacker: For overhearing technique, if node A sends a packet to node B and asks B to forward it to C, B would have many ways to make A believe that it has sent the packet to C, while actually it does not.
- Applicability: ESCT heavily relies on the dynamic information exchange between a source node and its former destination node(s) when they become direct neighbors so that possible malicious nodes in a route can be discovered.
- ESCT achieves a high PDR and throughput at the expense of increased normalized routing overhead and end-to-end delay.
- ESCT achieves a high PDR and throughput at the expense of increased normalized routing overhead and end-to-end delay.

4. PROPOSED METHODOLOGY

In Commerce settings P2P communities are often established dynamically with peers that are unrelated and unknown to each other. Peers of such communities have to manage the risk involved with the transactions without prior experience and knowledge about each other's reputation. One way to address this uncertainty is to develop strategies for establishing community-based trust through reputations [15, 16].

In a buyer-seller market, buyers are vulnerable to risks because of potential incomplete or distorted information provided by sellers. Trust is critical in such electronic markets as it can provide buyers with high expectations of satisfying exchange relationships. The basic idea is to detect and filter out exceptions in certain scenarios using cluster-filtering techniques.

The technique can be applied into feedback-based reputation systems to filter out the suspicious ratings before the aggregation. In comparison, our trust model is more general. We use the credibility of the feedback source as one of the basic trust parameters when evaluating the trustworthiness of peers. The credibility factor can be also used to detect fake or misleading ratings

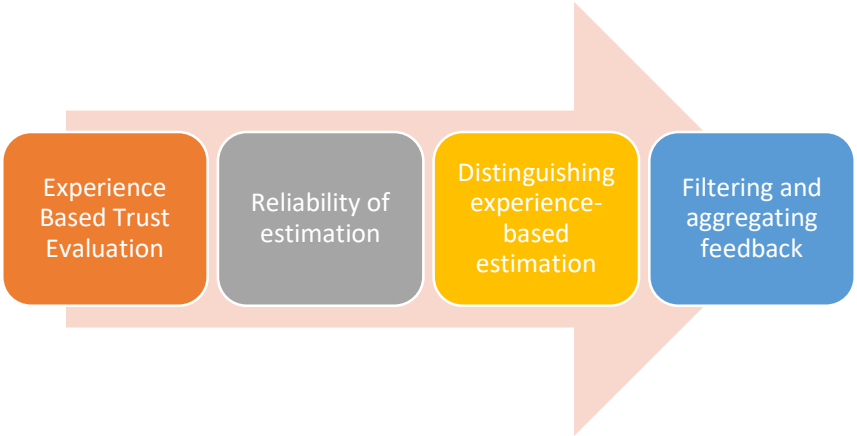

Fig. 4.1: - Proposed Methodology

4.1. Experience Based Trust Evaluation

The 'experience' component of trust for each node is directly measured by their immediate neighbours and kept updated at regular intervals in the trust table. The existing trust table is propagated to all other nodes as 'recommendation' part of the trust. At a regular interval, the previously evaluated trust is included in the current 'knowledge' component of total trust. Now either these three components individually or a combination of them can be used in computing the trust. All the nodes maintain neighbour table to keep information of frequently changing node and node trust value. Node trust value is evaluated using neighbour's collective opinion. The calculated trust value is stored in neighbour table corresponding to a node. Node trust is calculated by observing the behaviour of each node.

4.2. Reliability of Estimation

A node with a very low trust value is of little value to the system and depending on the application requirement may be evicted to prevent it from performing attacks to damage the system functionality. A node's trust value is assessed based on evidences such as direct observations as well as indirect recommendations. Our trust model is evidence-based. Thus we do not consider dispositional belief or cognitive characteristics of an entity in deriving trust. The trust assessment of one node toward another node is updated periodically.

4.3. Trust Aggregation

When the trust value on a particular target node propagated through multiple paths, multiple versions of this are received at the destination. Now the aggregation operation at the destination can combine these values together to obtain a single trust value [17]. Trust aggregation is based on the composability property of trust. The chain of nodes that transmits the trust information about target node to the trust requesting node constitutes a trust path. However, when the destination node receives trust value through multiple paths, if one path (e.g. the shortest) yields an unacceptably low level of trust, and other parallel paths yield better trust values, then they can be chosen based on the aggregation operations used. Hence, the aggregation can play important role in suppressing some of the malicious activities. The important factor to be considered for aggregation is the computational complexity. The nodes should be capable of executing the aggregation operations.

The proposed system consist of the following benefits,

- Most systems rely solely on the positive or negative feedbacks to evaluate and determine the reputation of peers. The feedback only approach suffers from inaccurate reflection of past experiences of peers in the respective community.
- Most systems assume feedbacks are honest and unbiased and lack ability to differentiate feedbacks obtained from less trustworthy peers and those from trustworthy peers.
- Most systems lack ability to set up various context sensitive feedback filters.
- Most systems lack temporal adaptively by either counting all the transaction history of a peer without decaying the importance of old transactions in the far past or only counts the recent transactions.
- Most systems do not provide incentives for a peer to rate others.

5. CONCLUSION

A trust metric model was developed to monitor misbehaving nodes in ad hoc routing protocol, their harmful influence was mitigated and they were avoided by nodes in selecting a reliable routing path. The model is believed to be simple and comprehensive in the way all the available information needed for calculating trustworthiness is gathered and used as appropriate. The model is totally decentralized and depends on the nodes experience gained in previous interactions, giving greater importance to recent experiences. Further, it has the ability to give another chance to misbehaving nodes to recover their trustworthiness values and come again to the network.

REFERENCES

[1] Lou, W., Liu, W., & Fang, Y. (2004, March). SPREAD: Enhancing data confidentiality in mobile ad hoc networks. In IEEE INFOCOM 2004 (Vol. 4, pp. 2404-2413). IEEE.

[2] Sankaran, K. S., & Hong, S. P. (2023). Trust Aware Secured Data Transmission Based Routing Strategy Using Optimal Ch Selection in Mobile Ad-Hoc Network. Mobile Networks and Applications, 1-13.

[3] Sankaran, K. S., & Hong, S. P. (2023). Trust Aware Secured Data Transmission Based Routing Strategy Using Optimal Ch Selection in Mobile Ad-Hoc Network. Mobile Networks and Applications, 1-13.

[4] Sathiyavathi, V., Reshma, R., Saleema Parvin, S. B., SaiRamesh, L., & Ayyasamy, A. (2020). Dynamic trust based secure multipath routing for mobile ad-hoc networks. In Intelligent Communication Technologies and Virtual Mobile Networks: ICICV 2019 (pp. 618-625). Springer International Publishing.

[5] Cho, J. H., Swami, A., & Chen, R. (2010). A survey on trust management for mobile ad hoc networks. IEEE communications surveys & tutorials, 13(4), 562-583.

[6] Awan, K. A., Din, I. U., Almogren, A., Kim, B. S., & Altameem, A. (2021). Vtrust: An iot-enabled trust-based secure wireless energy sharing mechanism for vehicular ad hoc networks. Sensors, 21(21), 7363.

[7] Alnumay, W., Ghosh, U., & Chatterjee, P. (2019). A Trust-Based predictive model for mobile ad hoc network in internet of things. Sensors, 19(6), 1467.

[8] Kumar, S., & Dutta, K. (2018). Trust based intrusion detection technique to detect selfish nodes in mobile ad hoc networks. Wireless Personal Communications, 101, 2029-2052.

[9] Vatambeti, R. (2020). A novel wolf based trust accumulation approach for preventing the malicious activities in mobile ad hoc network. Wireless Personal Communications, 113(4), 2141-2166.

[10] Ambekar, R. K., & Kolekar, U. D. (2022). T-TOHIP: Trust-based topology-hiding multipath routing in mobile ad hoc network. Evolutionary Intelligence, 15(2), 1067-1081.

[11] Sarbhukan, V. V., & Ragha, L. (2019). ETSR: enhanced trust based secure routing scheme for mobile ad hoc networks. Journal of Computational and Theoretical Nanoscience, 16(5-6), 2265-2272.

[12] VS, J., & MSK, M. (2018). Efficient trust management with Bayesian-Evidence theorem to secure public key infrastructure-based mobile ad hoc networks. EURASIP Journal on Wireless Communications and Networking, 2018, 1-27.

[13] Singh, U., Shukla, M., Jain, A. K., Patsariya, M., Itare, R., & Yadav, S. (2020). Trust based model for mobile ad-hoc network in Internet of Things. In Inventive Computation Technologies 4 (pp. 827-839). Springer International Publishing.

[14] Singh, K., & Verma, A. K. (2020). TBCS: A trust based clustering scheme for secure communication in flying ad-hoc networks. Wireless Personal Communications, 114, 3173-3196.

[15] Merlin, R. T., & Ravi, R. (2019). Novel trust based energy aware routing mechanism for mitigation of black hole attacks in MANET. Wireless Personal Communications, 104, 1599-1636.

[16] Velagaleti, S. B., GNITS S, S. M., & Raju, S. V. (2020). A novel method for trust evaluation in a mobile Ad Hoc network. Int J Comput Sci Inform Secur (IJCSIS), 18(2).

[17] Raja, R., & Ganeshkumar, P. (2018). QoSTRP: A trusted clustering based routing protocol for mobile ad-hoc networks. Programming and Computer Software, 44, 407-416.