A TRUST-BASED PREDICTIVE MODEL FOR MOBILE AD HOC NETWORKS

K.Divya[1] and Dr.B.Srinivasan[2]

[1]Ph.D Research Scholar, Department of Computer Science, Gobi Arts & Science College, Gobichettipalayam, India
[2]Associate Professor, Gobi Arts & Science College, Gobichettipalayam, India

ABSTRACT

The Internet of things (IoT) is a heterogeneous network of different types of wireless networks such as wireless sensor networks (WSNs), ZigBee, Wi-Fi, mobile ad hoc networks (MANETs), and RFID. To make IoT a reality for smart environment, more attractive to end users, and economically successful, it must be compatible with WSNs and MANETs. In light of this, the present paper discusses a novel quantitative trust model for an IoT-MANET. The proposed trust model combines both direct and indirect trust opinion in order to calculate the final trust value for a node. 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.

KEYWORDS

MANET, security, trust, ARMA, GARCH, clustering, IoT, predictive

1. INTRODUCTION

The Internet of things (IoT) is a heterogeneous network of physical devices, vehicles, home appliances, and other objects embedded with electronics, software, sensors, actuators, and connectivity. By enabling seamless connection between objects and the rapid exchange of large volumes of data, this paradigm offers a new class of advanced services characterized by being available irrespective of time, place, and person. The use of wireless networks makes the physical infrastructures smarter, secure, reliable, and the systems become fully automated. IoT collects, stores, and exchanges a large amount of heterogeneous data from different types of networks and provides critical services in healthcare, manufacturing, and utility networks.

Mobile Ad hoc Network (MANET) is a distributed collection of wireless nodes which can work without the presence of any centralized administration or fixed network infrastructure. In this network, the nodes are free to move randomly at any given time. In MANET, the nodes within the radio range can immediately communicate with each other, whereas the nodes that are not within each other's radio range are able to communicate with the help of intermediate nodes where the packets are relayed from source to destination.

Establishing secure communication in a MANET is particularly challenging because of

- Shared wireless medium
- No clear line of defense
- Self-organizing and dynamic network

- Most of the messages are broadcasted
- Messages travel in a hop-by-hop manner
- Nodes are constrained in terms of computation and battery power.

Trust can play an important role to improve security of ad hoc networks by a-priori or run-time evaluation of trustworthiness of its peers before making any routing decision.
Cryptographic mechanisms cannot help in order to detect/prevent such random behaviors which pose security threats to the network. The notion of trust management does not replace cryptography, but rather supplements to it. Cryptography and a trust decision framework can work hand-in-hand to achieve holistic security in IoT-MANET.

The term trust has been coined in the social science literature and adopted by distributed computing and mobile computing as well. Trust is a combination of opinion, belief prediction, and probability. Trust is a measurement of reliability, utility, and availability, and it also improves the overall network functionalities like quality of services, reputation, availability, risk, and confidence.

If the node believes that its peer would definitely not perform some action in any circumstance, the node does not "trust" the later again if it believes it would complete the particular task, the trust level is high. In both cases there is no uncertainty. But if the node is not confident about the next move of the other then uncertainty occurs. Unfortunately, nodes involved in IoT-MANET show this kind of uncertainty in their behavior. In the present proposal, the level of trust can be measured by a continuous real number, referred to as the *trust value*. Trust is not necessarily symmetric. The fact that A trusts B does not necessarily mean that B also trusts A, where A and B are two entities. As trust is subjective probability, when a system converges to a trusted stage it is not well addressed.

2. RELATED WORK

MANET has been well studied since the last decade. In recent years, the proliferation of the internet of everything concept increases the use and utility of MANET significantly. IoT-MANET is a budding topic because devices are wirelessly connected and most of them may be energy constrained, and networks are self-organized. Trust management schemes for MANET are the central point of attraction. We also discuss secure routing and trust propagation as well.

Most reputation-based trust management schemes are devised for collaborative secure routing by detecting misbehaving nodes that are either selfish or malicious. Upon designing secure routing protocols, researchers assumed a-priori trust relationships between mobile nodes. Proposed a trust based security architecture for key management in WANETs. The unique part of this work is that it considers the trust level of each node in a physical as well as a logical sense. Jiang and Baras addressed distributed trust computation and establishment using random graph theory and the theory of dynamic cooperative games. Liu et al. proposed an extension of AODV-based routing protocol B-AODV.

Where trust plays an important role to secure end-to-end delivery proposed a trust-based security architecture for key management in WANETs. The unique part of this work is that it considers the trust level of each node in a physical as well as a logical sense. Jiang and Baras addressed distributed trust computation and establishment using random graph theory and the theory of dynamic cooperative games. Liu et al. proposed an extension of AODV-based routing protocol B-AODV where trust plays an important role to secure end-to-end delivery.

3. PROPOSED WORK

A prediction-based trust management framework has been made to enable nodes to establish a trustworthy route and reliable data delivery in IoT-MANET.

- Number of packets properly forwarded (*Good*)
- Number of packets dropped (*Bad*)
- Number of packets falsely injected (*Bad*)

Trust calculations have been performed periodically, and after the expiration of each time period of the trust parameters are collected and direct observation is calculated by node.

3.1. Trust Revocation

This is the first phase when CH initiates the trust calculation of each member of the cluster. Due to the energy-constrained nature of IoT-MANET nodes, it is not appropriate to calculate trust at fixed intervals. Similarly, singleton trust generation is not good as the nodes are vulnerable to uncertain behavior due to the quasi-static nature (node mobility). The trust model is evidence-based, and it may change from time to time. This factor is application-specific and it can be set depending upon the requirement.

3.2. Trust Generation

In this phase, the trust value of each member of a cluster is evaluated. This phase is performed in two separate phases; direct trust (dir) calculation and resultant trust (res) generation. The detail procedure is described below. After calculating the trust value nodes are categorized.

3.3. Node Categorization

In MANET, a packet can be dropped by a node due to network congestion, link failures (node mobility) between nodes, network interference and contentions, selfishness (the nodes having limited energy saves their energy by not forwarding the packets), and maliciousness (the malicious nodes intentionally do not forward the packets). In an ideal scenario, the packets are dropped only due to maliciousness of a node. However in a real scenario, there are some inherent properties of the medium for which packets may be dropped, though the actual reason cannot be identified easily. Therefore, we define a “bad node” as a node that randomly drops packets deliberately.

3.4. Trust Propagation

Once the resultant trust of each member node is finalized, in this phase CH propagates these values to the other cluster members.

3.5. Routing

For creating routes between source and destination, maintaining the routes and the network, the proposed routing needs to perform the following three phases.

- **Neighbor Discovery**

This phase is responsible for maintaining the list of trusted neighbors, along with their trust status.

- **Route Discovery**

In this phase the end-to-end path is established by including only good and uncertain nodes.

- **Route Maintenance**

This phase maintains the established route. Each node on an active path monitors the link periodically. It also revokes the route discovery phase if link failure occurs due to node mobility.

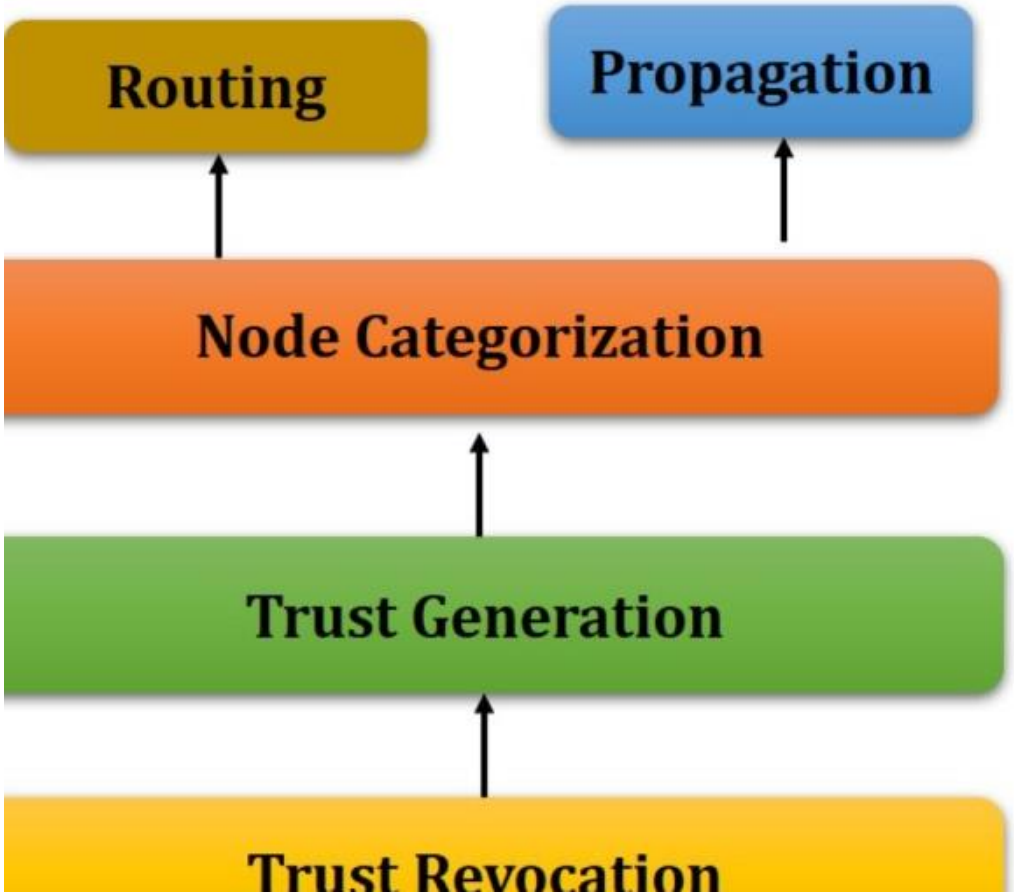


Figure 1. Trust Model

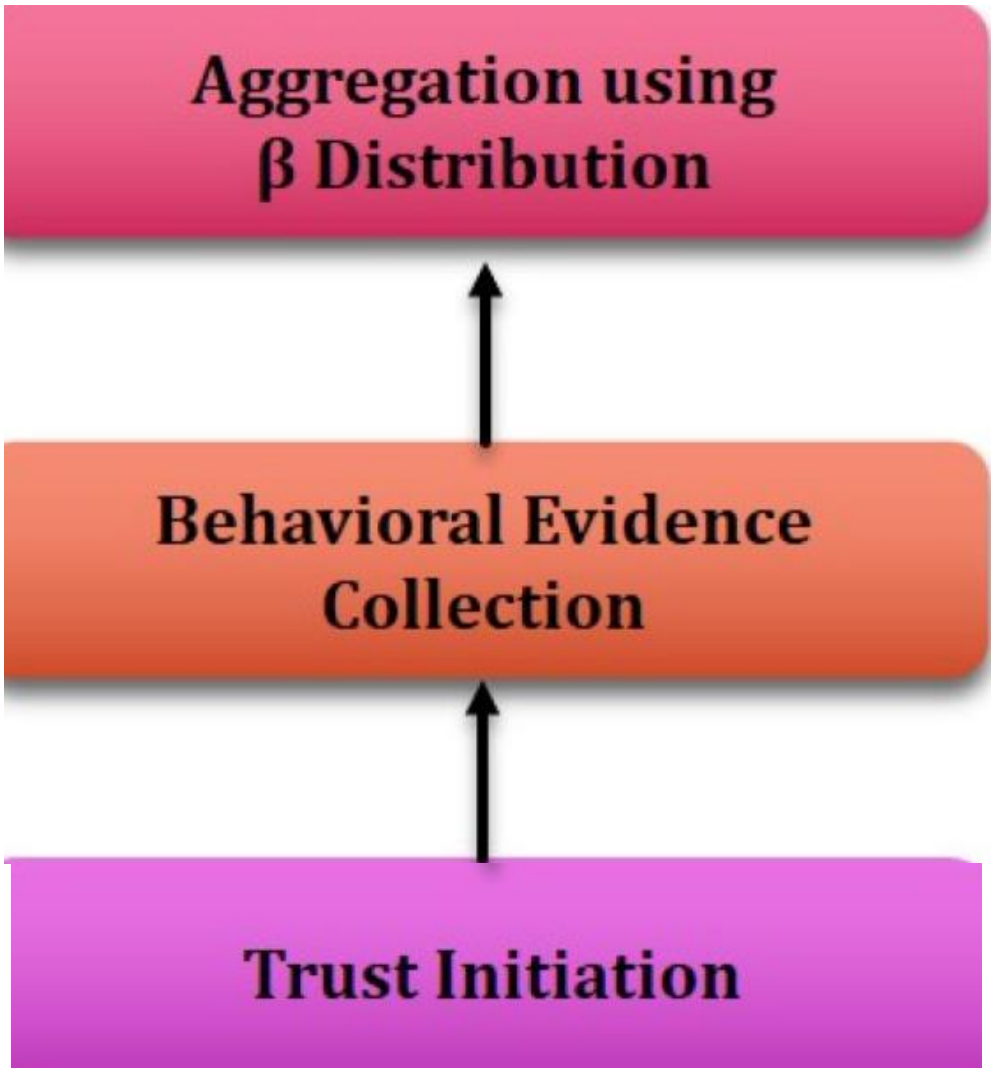


Figure 2. Trust Generation

3.2. Trust Generation

Trust generation has been achieved in two steps; direct trust calculation and resultant calculation.

3.2.1. Direct Trust Calculation

- **Trust Initiation**

Along with bootstrapping the IoT-MANET, CH and cluster members initiate the trust calculation. Once the trust value has aged, the trust revocation procedure is restarted and the direct trust calculation takes place.

- **Evidence Collection**

In this phase both CH and cluster members collect the *Good* and *Bad* evidences, as described

- **Trust Aggregation**

In this phase each member and CH of a cluster collects and stores collective data for all good and bad events. A reputation system-based on the β probability density function has been used, in order to calculate direct trust. The β function represents probability distributions of binary events (either good or bad).

3.2.2. Resultant Trust Generation

- **Neighbor Management**

Each member of a cluster (including CH) maintains a list of neighboring nodes. CH broadcasts *Hello* messages periodically and maintains a list of node-IDs of members in the cluster. Each member also exchanges *Hello* messages periodically to keep track of its neighbors.

- **Trust Information Collection**

Here, CH collects the recommendation from common neighbors to compute the resultant trust of a node under review.

- **Trust Aggregation**

On receiving the recommendation of trust evidences from the members, CH executes ARMA (1, 1)/ GARCH (1, 1) to calculate the resultant (or final trust) of a node under review. The resultant trust of a node can be calculated using ARMA

$$Xt = \varepsilon t + \Sigma pi=1 \varphi i Xt-i + \Sigma pi=1 \theta i Xt-i$$

4. SIMULATION

Here, the direct trust of a node is calculated by monitoring its behavior and collecting information about the node. It chooses different parameters (such as the number of packets forwarded, dropped, misrouted, and falsely injected) for the direct trust calculation. CH periodically collects the direct trust values of member nodes and uses the modified Dempster–Shafer theory to compute the global trust value of a node. In our present work, the direct trust is calculated using a quantitative model by taking into consideration the trust parameters which are combined by the β distribution. In order to calculate the resultant trust value of a node under consideration, various recommendations are collected and combined using the ARMA/GARCH model.

4.1. Simulation Parameters

The transmission range of each node is set to 250 m. The nodes travel with a speed varied from 0 m/s to 5 m/s, with a pause time set to 5 s. A cluster may get partitions very frequently due to high node mobility. All the trust-based protocols, including our proposed protocol, may not be suitable in highly dynamic networks. UDP has been used as the transport layer protocol with constant bit rate (CBR) traffic generator of packet size 512 bytes. Simulation has been performed for 500 s with a 21-node cluster over a network area of 450 m × 450 m. The proposed trust protocol is based on a 1-hop cluster and hence the network area is chosen to be 450 m × 450 m. The malicious nodes drop the packets randomly whereas the good nodes drop the packets due to the environment of the network (such as mobility of nodes, collisions of packets, etc.) in our simulation.

4.2. Detection Ratio

To evaluate the accuracy of the proposed trust model, false positive is chosen as the performance metric. False positive is measured as the ratio of the number of good nodes falsely detected as malicious to the total number of nodes in the network. The percentage of packet collision versus percentage of false positive of the proposed trust model. From the graph it is evident that only 5% nodes are wrongly detected as malicious when 24.78% and 23.36% packet collisions occur for *Low* level and *High* level, respectively. Again, the proposed trust model falsely detects nearly 24% nodes as malicious when 49.32% and 47.93% packet collisions take place for *Low* level and *High* level, respectively. Therefore, the proposed trust model performs well even when the rate of packet collision in the network is high.

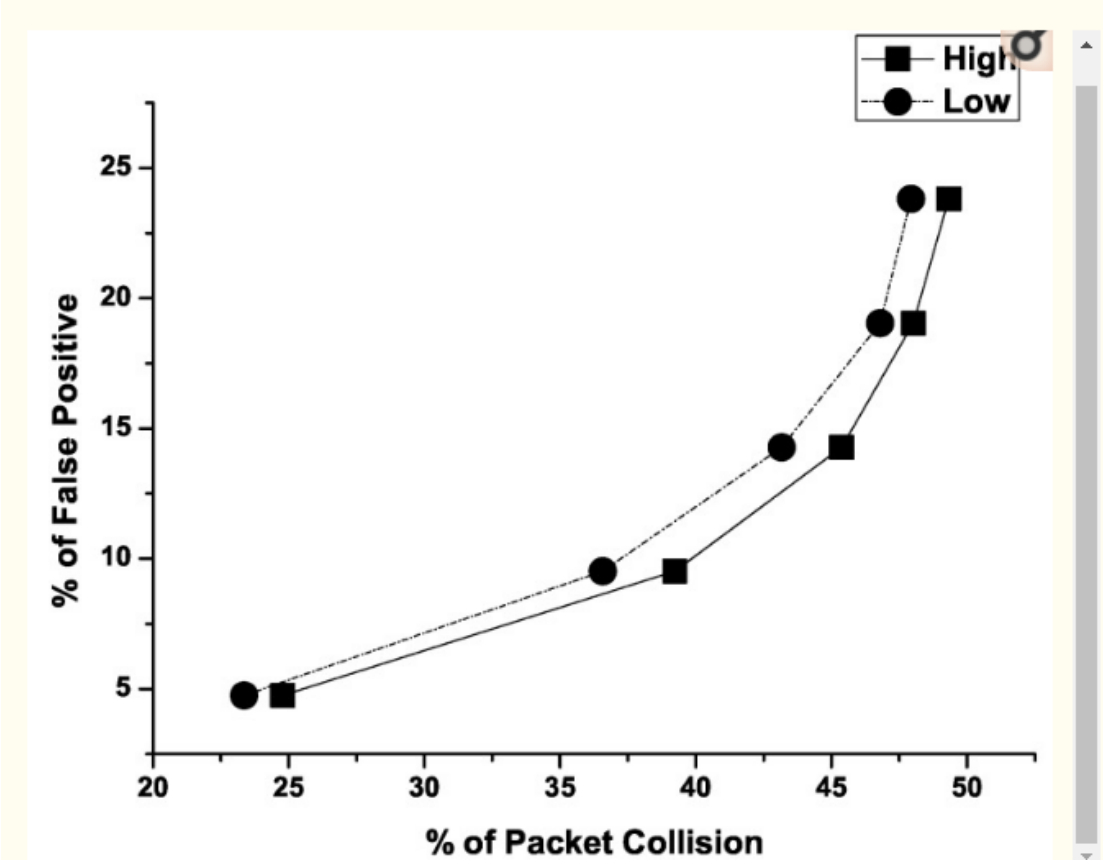


Figure 3. False Positive Vs Packet Collision

4.3. Performance Evaluation

We considered four parameters, packet delivery fraction (PDF), packet drop rate (P Drop R), packet delivery ratio (P Del R), and throughput (THR), as performance metrics in order to compare the proposed trust-based routing protocol with two existing and well-studied protocols.

It is evident that the packet delivery fraction is more than 0.9 in the absence of malicious nodes for all schemes. However, P Drop R increases and subsequently PDF decreases with the increased number of malicious nodes for all the protocols. CBRP gives 0.61 and 0.12 as PDF when nearly 5% and 25% malicious nodes are present in the network, respectively. The protocol

proposed by Chatterjee et al. offers 0.71 and 0.27, whereas our proposed protocol gives 0.77 and 0.42 as PDF for the same percentages of malicious nodes.

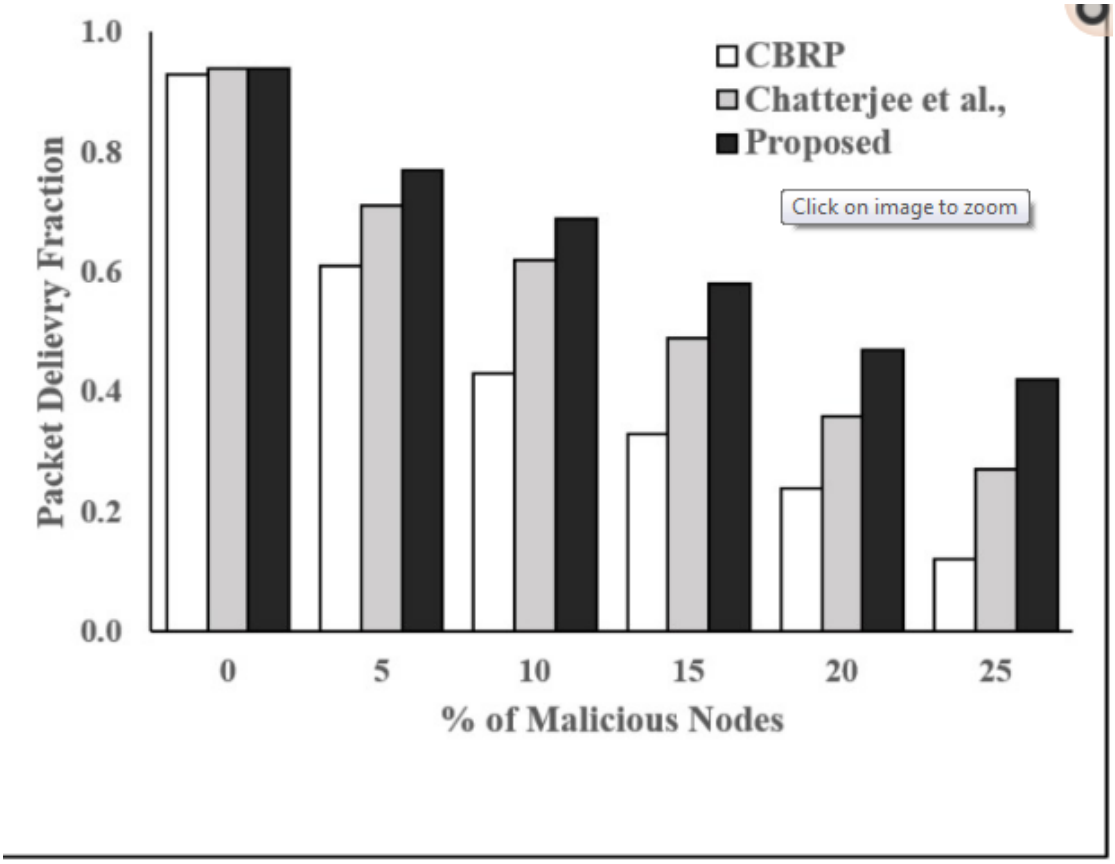


Figure 4. Packet Delivery Fraction Vs Malicious Nodes

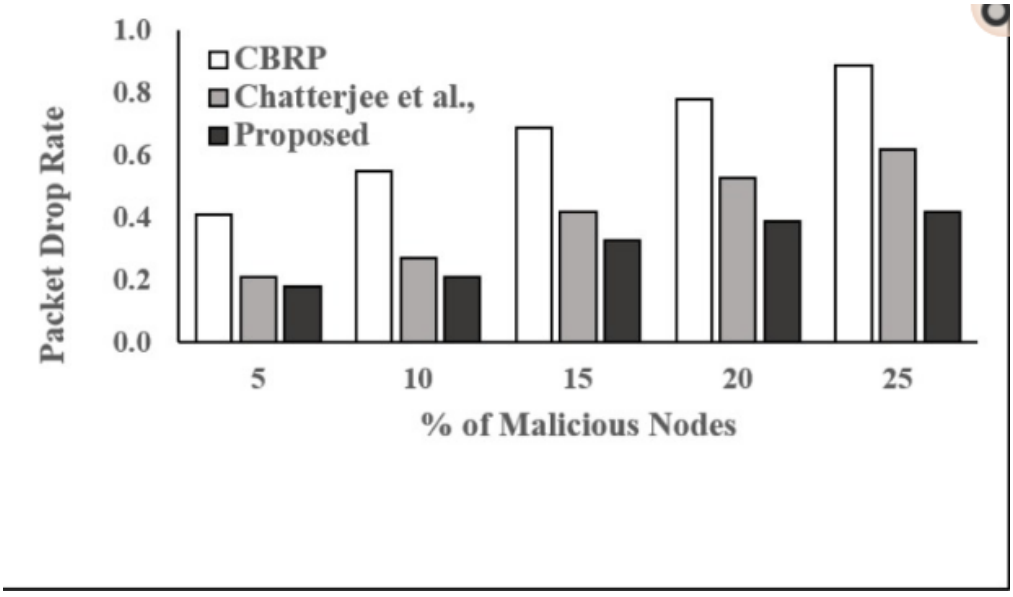
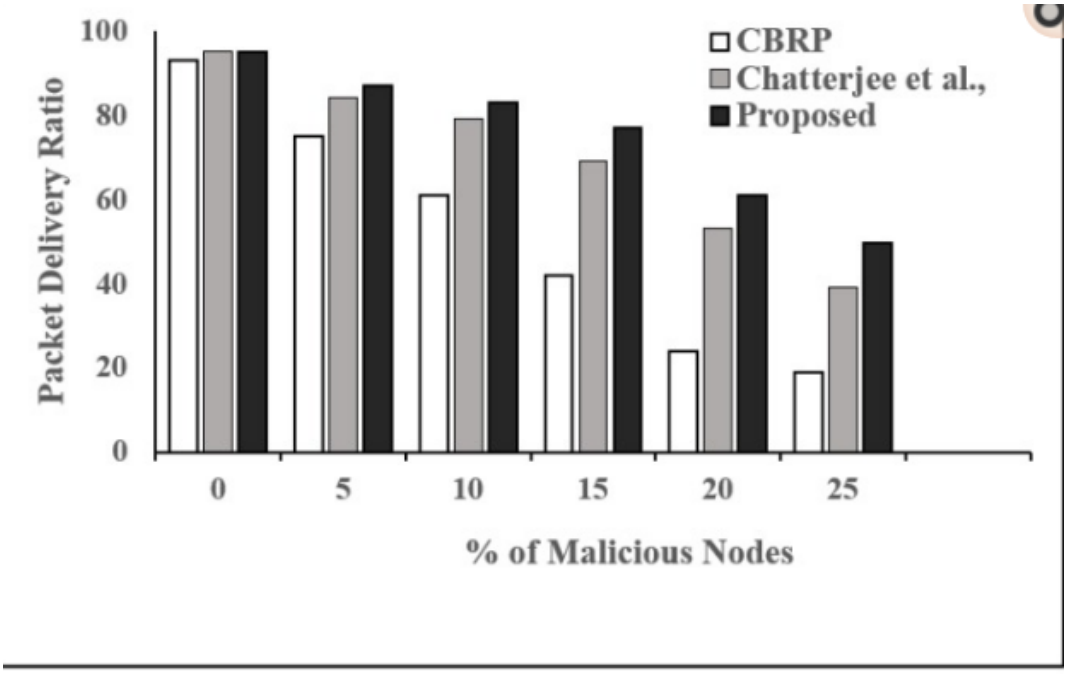


Figure 5. Packet Drop Rate Vs Malicious Nodes

CBRP, P Drop R increases from 0.41 to 0.89 when the number of malicious nodes increases from about 5% to 25%. It is evident that the proposed protocol outperforms the protocol proposed by Chattejee et al. and CBRP. This is due to the fact that our proposed protocol can predict the trust value of a node at least one step ahead and provides trustworthy routes between source and destination.



All the protocols give around 93% P Del R when none of the nodes are malicious. Due to the absence of security mechanisms in CBRP, the P Del R reduces to 19% in the presence of 25% malicious nodes. Though Chatterjee et al. consider the security aspects (trust) while setting up the route, the proposed protocol outperforms the other two protocols and gives around 50% PDR even when 25% of the nodes behave maliciously.

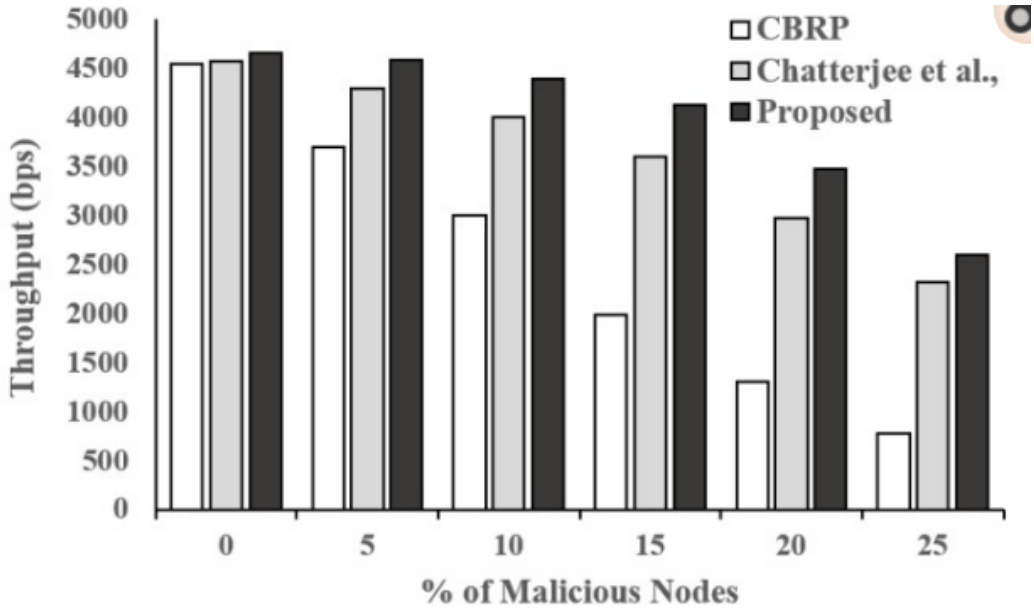


Figure 7 Throughput Vs No of Malicious Nodes

It can also be seen that the proposed protocol outperforms the other protocols in the presence of malicious nodes. In the presence of 25% malicious nodes, the proposed scheme gives throughput around 2600 bps whereas CBRP and the protocol proposed by Chattrejee et al. offer throughput around 800 bps and 2300 bps, respectively.

5. SECURITY ANALYSIS OF PROTOCOL

In this section, we discuss the attack model for the proposed protocol. The trust model runs in real time and the malicious (i.e., dropped or falsely injected packets) can be detected on-the-fly and isolated as a *blacklisted* node.

- **Address Spoofing**

In this attack, the attacker tries to spoof an address (that is IP and ID) of a victim node. Using a one-way secure hash function the present scheme can prevent the attacker from stealing the ID/IP of a node. Moreover, the attacker cannot generate the signature of the victim node.

- **Routing Table Overflow and resource consumption attacks**

In the proposed model, trust is calculated real time and nodes are being monitored for their functionality in order to calculate trust. Thus, any compromised or malicious attacker generating overflow or resource consumption can be detected.

- **Byzantine/ Black hole/ DoS Attack**

During node monitoring, if a node finds another neighbor sending packets to a particular node repeatedly, dropping packets, or holding the packet more for than a certain interval, a *Warning* message is generated and temporarily restricts other good nodes from communicating with the suspicious node until the next review comes.

6. CONCLUSION

In this paper, a novel quantitative trust model for a clustering environment in IoT-MANET has been proposed. The prediction-based trust model can collaboratively compute the resultant trust of a node using direct trust and recommendation trust opinions from other nodes. The proposed evidence-based trust model utilizes the probabilistic model of β distribution to calculate the direct trust of a node under review. From the resultant or final trust of the node under review, the theory of ARMA/GARCH has been used to predict the future behavior of the node, which is derived from its past behavior. Using a weighted combination model, the direct trust evidence and collected recommendation evidences are combined so that the effect of malicious reporting can be minimized. Extensive simulation study shows that the model outperforms the similar trust-based protocols in terms of false positive detection, even for a highly congested network.

The proposed trust model can be applied in IoT-WSN and subsequently in smart cities to provide security. Further, it can provide security in software-defined mobile ad hoc networks (SD-MANET), where SDN controllers can collect the recommendation trust and compute the resultant trust value of their nodes.

REFERENCES

[1] Gambetta D, (2000), "*Trust: Making and Breaking Cooperative Relations*", Basil Blackwell, Oxford, UK pp. 213–237.

[2] Wang X, Liu L, Su J. Rlm, (2012)," *A general model for trust representation and aggregation*", IEEE Trans. Serv. Comput, 2012;**5**:131–143.

[3] Pham H.T, Yang B.S, (2010),"Estimation *and forecasting of machine health condition using ARMA/GARCH model*", Mech Syst Signal Process, 24:546–558.

[4] Velloso P, Laufer R, de O Cunha D, Duarte O, Pujolle G, (2010),"*Trust management in mobile ad hoc networks using a scalable maturity-based model*", IEEE Trans. Netw. Serv. Manag, 7:172–185.

[5] Jain S, Baras J, (2013)," *Distributed Trust Based Routing in Mobile Ad-Hoc Networks*", Proceedings of the IEEE Military Communications Conference (MILCOM); San Diego, CA, USA. 18–20 November 2013; pp. 1801–1807.

[6] Desai A, Jhaveri R, (2019)," *Secure routing in mobile Ad hoc networks: A predictive approach*", Int. J. Inf. Technol **11**:345–356.

[7] Ghosh U, Datta R, (2015)," *A Secure Addressing Scheme for Large-Scale Managed MANETs*", IEEE Trans. Netw. Serv. Manag, **12** 483–495.

[8] Rath M, Panigrahi C.R, (2016),"*Prioritization of Security Measures at the Junction of MANET and IoT*", Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, Udaipur, India. 4–5 March 2016; pp. 1–5.

[9] Chiang C.C, Wu H.K, Liu W, Gerla M,(1997)," *Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel*",Proceedings of the IEEE Singapore International Conference on Networks; Singapore. 14–17, pp. 197–211

[10] Dempster A.P, (2015)," A generalization of Bayesian interface", *J. R. Stat. Soc.***30**:205–447.

[11] Josang A, Ismail R, Boyd C,(2007)," *A survey of trust and reputation systems for online service provision*", Decis Support Syst **43**:618–644.