Fuzzy Model for Intrusion Detection using Trust System based Bias Minimization & Application Performance Maximization In MANET

Pradnya M. Nanaware
Sinhgad Institute of Technology,
Lonavala,Pune.
Savitribai Phule Pune University,
Pune, India

Sachin D. Babar, PhD
Sinhgad Institute of Technology,
Lonavala, Pune.
Savitribai Phule Pune University,
Pune, India

ABSTRACT
The mobile ad-hoc network (MANET) contains various types of mobile nodes. The Trust of the node is an important issue for deciding the behavior of the node. The behavior of the node is in terms of maliciousness of the node. Trust management for MANETs is an active research area. MANET is a collection of nodes that are self-configuring. There is the absence of any centralized control. In MANET, any node can enter and exit from the communication. This paper addresses the performance issue of trust management. Trust management deals in two important areas :trust bias minimization and application performance maximization The paper helps to implement the best trust protocol settings for minimized trust bias and maximize application performance. This paper helps to minimize the trust under the presence of malicious nodes.

Keywords
Communication, MANET, QoS, Trust management, malicious, Trust bias minimization

1. INTRODUCTION
The idea of "trust" is a subjective level of conviction about the practices of a specific element. "Trust administration helps for determining and translating security approaches, qualifications, and connections." Experts have characterized trust contrastingly, for example, "a conviction on unwavering quality, reliability, on the other hand, security", "a conviction about capability or genuineness in a particular connection", and "dependability, opportunity, and uprightness of message conveyance" [1]. Trust administration can be used for secure directing, key administration, verification, and access control and interruption recognition [2]. Trust administration for portable impromptu systems (MANETs) has developed as a dynamic exploration region as prove by the expansion of trust conventions to bolster versatile gathering based applications in later a long time. This paper addresses the execution issue of trust administration convention outline for the MANET in the two critical territories: trust inclination minimization and execution of the application.

The proposed trust management protocol is dependent on trust metric such as social and QoS. This protocol helps to yield end-to-end subjective trust evaluation. The MANET comprises human operators using communication devices. Thus in addition to traditional QoS trust metrics such as control packet overhead, throughput, packet dropping rate, availability. The social trust metrics plays an important role as human operators are involved in the system. The proposed work identifies the suitable trust aggregation parameter settings for the operator's trust metric to minimize trust bias. The trust metrics are the quality of service and social trust.

The node behavior is studied in the presence of various scenarios such as well-behaved nodes and malicious nodes. This approach helps to decide the desired trust parameter settings. These settings help to set the SQ Trust more accurately on global information and actual node status.

This paper is arranged in this manner. Section 2 discusses related work; Section 3 discusses Manet and Trust Management, Section 4 discusses the generic architecture of the proposed topic .Section 5 describes conclusion and future scope.

2. RELATED WORK
The related work is an existing work done in the field of trust management in MANET.

F. Bao et al. [3] demonstrated a cluster-based trust management protocol for WSNs. The proposed protocol is cluster based. Authors have considered multidimensional trust traits determined by correspondence and informal organizations to assess the trust of a sensor hub. Using novel likelihood model, authors have portrayed a heterogeneous WSN involving an extensive number of sensor hubs with limitlessly diverse social and nature of administration practices with the goal to yield "ground truth" hub status.

M. Blaze et al. [4] have explained the importance of trust management in the network. The authors have focused on trust as a distinct and important component of security in network and services. The trust management problem includes formatting security policies and security credentials. Determining whether a particular set of credentials satisfy the relevant policies and deferring trust to a third party. The trust management helps to verify the existing systems that help security in network applications, including X.509 and PGP. The authors have given a comprehensive approach for trust management specifying the trusted actions and trust relationship.

B. J. Chang et al. [5] have explained MANETs are resource constraint and vulnerable to various security attacks. Trust-based security modeling to go hand in hand with cryptographic services to offer good security services. This paper thus proposes a two-step secure authentication approach for multicast MANETs. The two-step secure authentication helps to ensure the more security. A Markov chain trust model is used to calculate the trust value (TV) for each one-hop neighbor. The node with the highest TV in a group will be selected as the Certificate Authentication (CA) server.

Y. Ren et al. [6] have proposed a human-based model that assembles a trust relationship between hubs in an impromptu

system. The trust depends on past individual encounters also, on the proposals of others. A reputation-based trust system is able to track the behavior of nodes. The system rewards well-behaving nodes and punishes misbehaving ones.

J. H. Cho et al. [7] have explained that the Portable Ad Hoc Network (MANETs) is a Collection of versatile hubs joined with remote connections. The authors have given the detailed survey of the trust management in MANET. The trust depends on various factors of the nodes. The unique characteristics of the trust are derived with the help of the social notions of the trust. MANET has no altered topology as the hubs are moving continually shape one spot to somewhere else. All the hubs must co-work with one another keeping in mind the end goal to course the bundles. Participating hubs must trust one another. Accordingly trust is an essential word that influences the execution of MANET. There are a few conventions proposed given the trust. This paper is a review of trust based conventions, and it proposes some new procedures for trust administration in MANETs.

3. MANET AND TRUST MANAGEMENT

The MANET is an autonomous transitory association of mobile nodes that communicate with each other over wireless links[6]. Nodes that lie within each others send range can communicate directly and are responsible for dynamically discovering each other. Devices are free to join or leave the network and they may move randomly, possibly resulting in rapid and unpredictable topology changes.

Trust is dynamic; it evolves with time, experience and the environment. The maliciousness depends on the trust on the particular node. The more trusted nodes are more reliable for the communication and quality of the system. The overall quality of the network is dependent on the social behavior of the node [8]. The previous work shows that trust can be an important factor for selecting the valid node.

The trust-based routing is helpful for proper communication and intrusion detection. The node that has lower trust value cannot be considered for the communication as the probability of the attack may increase. The performance of the node decides the overall performance of the network. Hence, it is important to have more trusted nodes in the network. More the trusted nodes in the network better the performance and quality of the network. The trust of the node depends on various parameters of the nodes such as social behavior, authentication, reliability, maliciousness of the node. Different parameters are considered to decide the trust value for the node.

The analysis of the various research works shows the importance of trust management and the effect of trust on the network.

4. PROPOSED WORK

The proposed system will be a mechanism for Intrusion Detection Using Trust System Based Bias Minimization and Application Performance Maximization in MANET. The system will detect the intrusion from the network depending on the trust of the particular node [9]. The proposed work consists of Simulation based approach. Trust management framework covers all the aspects of trust management namely trust composition, trust aggregation, trust formation.

4.1 Trust Composition

Trust metric consist is of two types of trust: social trust and QoS trust. Social trust is evaluated through interaction experiences in social networks to account for social relationships [10]. Among the many social trust metrics such as friendship, honesty, similarity and social ties. Many QoS metrics such as competence, cooperation, reliability. Competence (measured by energy) and protocol compliance (measured by cooperativeness in protocol execution) to measure the QoS trust level of a node.

4.2 Trust Aggregation

A proposed trust aggregation protocol design discovers and applies the optimal trust parameter settings to reduce the subjective trust and objective trust differences. Node i will compute its trust toward Node j, $T^X_{ij}(t)$,where X is a trust component by:

$$T^X_{ij}(t) = \beta_1 T_{ij}^{direct,\,X}(t) + \beta_2 T_{ij}^{indirect,\,X} \quad (1)$$

In Eq.(1), β1 is a parameter to weigh node i's own information toward node j at time t, i.e.,''direct observations'' and β2 is a parameter to weigh indirect information from recommenders, i.e., ''information from others,'' with $\beta_{1+}\beta_2 = 1$.

Node i will compute $T_{ij}^{direct,\,X}(t)$ by :

$T_{ij}^{1\text{-}hop,X}(t)$ if i is a neighbor to j at t

and data needed is obtainable.

$T_{ij}^{direct,\,X}(t) =$

$e^{-\lambda\Delta t} \times T_{ij}^{direct,\,X}(t-\Delta t)$ Otherwise (2)

In Eq.(2), To account for trust decay over time, we adopt an exponential time decay factor, $e^{-\lambda\Delta t}$ to satisfy the desirable property that trust decay must be invariable to the trust update frequency.

Node i will compute $T_{ij}^{indirect,\,X}(t)$ by :

$$T_{ij}^{indirect,\,X}(t) = \begin{cases} \dfrac{\sum_{mv}\left(T_{i,m}^{X}(t) \times T_{m,j}^{direct,X}(t)\right)}{e^{-\lambda\Delta t} \times T_{ij}^{direct,\,X}(t-\Delta t)} & \text{if } n_r > 0 \\ e^{-\lambda\Delta t} \times T_{ij}^{direct,\,X}(t-\Delta t) & \text{if } n_r = 0 \end{cases} \quad (3)$$

In Eq.(3), the trustor node (node i) first selects n_r recommenders (node m's) with which it trusts the most in trust component X among its one-hop neighbors and then requests these recommenders to send their recommendations.

4.3 Trust Formation

Proposed work defines trust parameters used for trust formation protocol design. The importance-weighted-sum model is adopted. Specifically node i will compute $T_{ij}(t)$ by :

$$T_{ij}(t) = \sum_X W^X \times T^X_{ij}(t) \quad (4)$$

In Eq.(4), $T_{ij}(t)$ is the trust belief of node i toward node j in trust component X = intimacy, healthiness, energy or cooperativeness and w^x is the weight associated with X. Below we use the notation w1:w2:w3:w4 for $w^{intimacy}$:$w^{healthiness}$: w^{energy} :$w^{cooperativeness}$ for notational convenience. Intimacy trust is an aggregation of direct interaction experience ($Tij^{direct,\,intimacy}(t)$) and indirect interaction experience ($T_{ij}^{indirect,\,intimacy}(t)$). Place Energy represents the current energy level of a node.

4.4 Methodology

Calculate direct and indirect trust. It is input to the trust formation process.Output of this process is Subjective and Objective trust .Calculated trust value T_{ij} is input to Fuzzy logic. In rule set generation define membership function (range).Range define for energy, healthiness trust parameter is 0 to 10.Then use Fuzzification and Defuzzification process. Fuzzification is process of making a crisp quantity fuzzy. Defuzzification is conversion of a fuzzy quantity to a precise quantity.Calculate the throughput ratio. Value of throughput

ratio lies between 0-1.Dependability metrics such as availability , percentage of malicious nodes , result of Intrusion Detection and fault tolerance based on reputation thresholds also have been employed .

Measures are used for trust evaluation in MANET such as Throughput, Delay and Detection Ratio. Threshold values are choosing based on behaviour of the n/w and attack. Throughput is the rate of successful message delivery over a communication channel. Delay specifies how long it take for a bit of data to travel across the network from one node or endpoint to other. The performance of the network depends on the behavior of the nodes in the network. Trust value accuracy is important to decide the behavior of the node. Intrusion detection ratio is calculated and used to decide the amount (in %) of intrusion detection in the network.

4.5 Algorithm

Step 1: Input simulation topology parameters

Step 2: Create network toplology

Step 3: Join group

Step 4: Trust formation

Step 5: Calculate subjective and objective trust

Step 6: Trust aggregation and bias minimization

Step 7: Mission reliability (find the malicious node)

Step 8: Mission failed then exit

Step 9: Otherwise continue from step 4

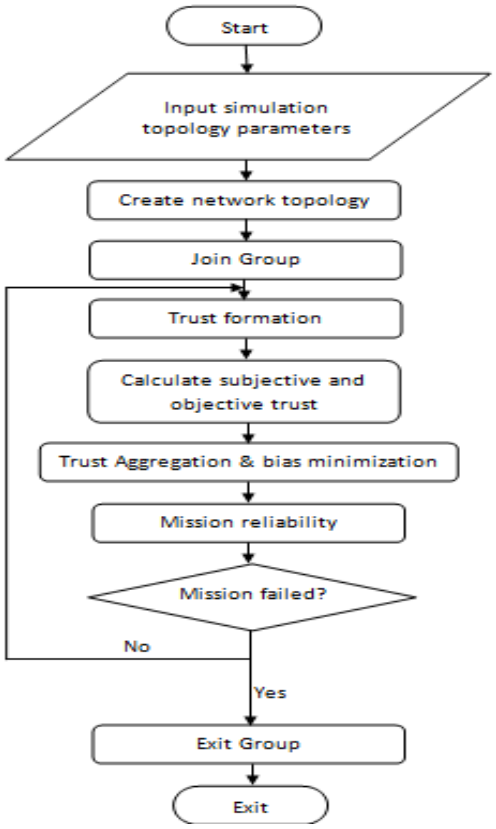

Figure 1 Generic Model

Figure 1 shows the generic model for the proposed system. With the implementation of the proposed system, the various disadvantages related to trust issues in MANET can be reduced.

5. CONCLUSION AND FUTURE SCOPE

This paper is focusing mainly on trust bias minimization and application performance maximization. The survey shows how the trust is important for deciding the behavior of the node in the network. The trust value is an important parameter to decide the maliciousness of the node. The higher trust value shows more confidence in the particular node.

In future, the various trust parameters can be considered for improving the trust factor. The trust value for a particular node can be calculated by considering some network scenarios. The various network scenarios will help to develop the most sustainable system for trust management. More than one parameter can be considered for detecting the malicious activity in the network.

6. REFERENCES

[1] Ing-Ray Chen, Jia Guo, Fenye Bao, Jin-Hee Cho, "Trust management in mobile ad hoc networks for bias minimization and application performance maximization", Elsevier 2014.

[2] Rajshree Ambatkar, Purnima Selokar, "A Literature Review of Enhancing Security in Mobile Ad-Hoc Networks Using Trust Management Security Scheme", IJSR Volume 3 Issue 12, December 2014.

[3] F. Bao, I.R. Chen, M. Chang, J.H. Cho, "Trust-based intrusion detection in wireless sensor networks", in: IEEE Int'l Conf. on Communication, Kyoto, Japan, June 2011, pp. 1-6

[4] M. Blaze, J. Feigenbaum , J. Lacy, "Decentralized trust management", in: IEEE Symposium on Security and Privacy, May 1996, pp. 164-173.

[5] B.J. Chang, S.L. Kuo, "Markov chain trust model for trust value analysis and key management in distributed multicast MANETs", IEEE Trans. Veh. Technol. 58 (4) (2009) 1846-186

[6] Y. Ren, A. Boukerche, "Modeling and managing the trust for wireless and mobile ad-hoc networks", in: IEEE International Conference on Communications, Beijing, China, May 2008, pp. 2129-2133.

[7] J.H. Cho, A. Swami, I.R. Chen, "A survey on trust management for mobile ad hoc networks", IEEE Commun. Surv. Tutorials 13 (4) (2011) 562-583.

[8] Jin-Hee Cho,"Integrated Social and Quality of Service Trust Management of Mobile Groups in Ad Hoc Networks" U.S. Army Research Laboratory.

[9] C. Ashok Baburaj, Dr. K. Alagarsamy, "Repetitive Trust Management and Adversary Detection For Delay Tolerant Networks", JATIT 2014.

[10] E.M. Daly, M. Haahr,"Social network analysis for information flow in disconnected delay-tolerant MANETs", IEEE Trans. Mob. Comput. 8 (2009)606-621.

[11] Younghun Chae, Lisa Cingiser DiPippo,Member, IEEE Computer Society," Trust Management for Defending On-Of Attacks",April 2015.

[12] Xiaoyong Li, Feng Zhou, and Junping Du,LDTS:" A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks",June 2013.