Grenze International Journal of Engineering and Technology, Jan 2017

Layered Structure Implementation Model for Trust based System Design in MANETs

Renu Popli[1], Dr. Kanwal Garg[2] and Sahil Batra[3]
[1]Ph.D. Scholar, DCSA,KUK
renu_popli@yahoo.co.in
[2]DCSA,KUK
gargkanwal@gmail.com
[3]GIMT,Kanipla
sahil.batra23@gmail.com

***Abstract*—Mobile Ad-hoc networks are extremely susceptible to various misbehaviours and a variety of trust management schemes have been proposed to detect and mitigate them. Trust computation and management are highly challenging issues in MANETs due to computational complexity constraints, and the independent movement of component nodes. Here an implementation based layered model for trust is proposed. The main goal is to cover all the questions that a programmer needs to design a trust based system. The model is divided into three layers which are data collection, trust calculation and application layer. Each layer has its specific functions which work in integrating manner with another layer in order to build a complete system.**

***Keywords*: Mobile Ad-hoc Networks, Trust Management, Cryptography, Security, Fuzzy.**

I. INTRODUCTION

MANET is an infrastructure-less network of mobile nodes. In this type of networks, every node is self-maintained and there is no any centralized management. It's difficult to achieve security in MANETs due to vulnerability of the wireless link, absence of centralized management authority and dynamically changing topology. Distributed collaborations and information sharing are considered to be essential operations in the MANETs. Collaboration will be productive only if all participants operate in a cooperative manner.

Trust is the belief level [8] that one node can put over another node for a specific action based on direct and indirect observations on behaviours of that node. The node in a network evaluates trust for another participating nodes and then form the trust relation between them. Trust management framework is the framework to manage this kind of relations.

II. CHARACTERSTICS OF TRUST IN MANETS

Due to the unique characteristics of MANETs and inherent unreliability of the wireless medium, the concept of trust in MANETs should be carefully defined. The main features of trust in MANETs are as follows [4]:

1) A trust decision framework for MANETs should not assume that all nodes are cooperative.
2) Trust is dynamic, not static.

Grenze ID: 01.GIJET.3.1.50

3) Trust is subjective.
4) Trust is not necessarily transitive. The fact that A trusts B and B trusts C does not imply that A trusts C.
5) Trust is asymmetric and not necessarily reciprocal.
6) Trust is context dependent.

III. Trust Definitions

Trust is an abstract concept. There are several definitions given to trust in literature in various areas like sociology, psychology, e-commerce etc. but none of those can correctly describe the definitions of trust. Trust can be judged by different concepts like reliability, utility, availability, reputation, risk, confidence and other concepts [3].

With respect to MANET sense, these definitions can be classified into following:

1) *Trust as risk factor*: the definition given by Morton Deutch [6] states that trusting behaviour individual perceives an ambiguous path, the result of which could be good or bad, and the occurrence of the good or bad result is contingent on the actions of another person.
2) *Trust as belief*: trust is an individual's belief and willingness to act on the basis of words, actions and decisions of another.

IV. A Layered Implementation Model For Trust Based System

This section includes the answers to the various questions that arises in the mind of a trusted system developer while developing the system. Basically the whole process of trust based system design is divided into 3 layers as shown in figure below:

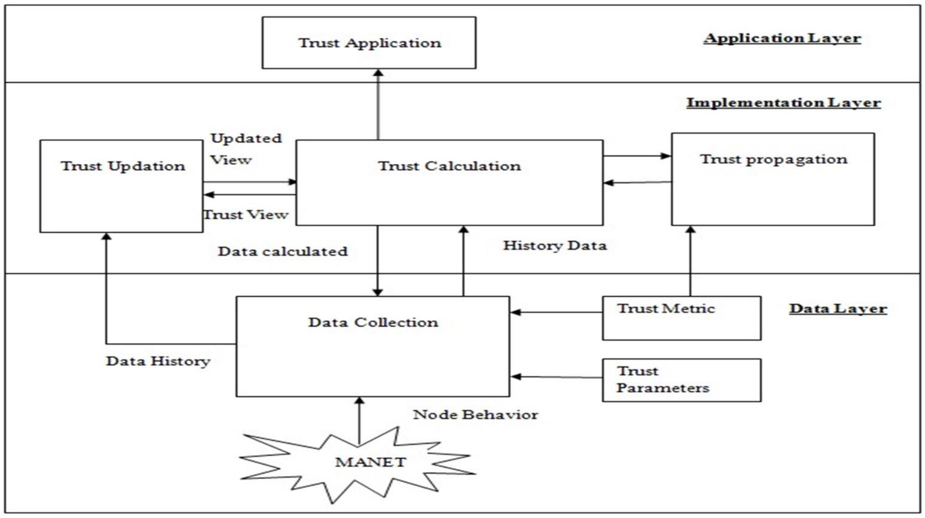

Figure 1: layered structure model for trust based system design

The basic process of designing includes the following: first of all data is collected from the behaviour of the nodes in MANETs. After collecting the data trust value of the nodes will be calculated based on some parameters using some metrics. This trust calculation can be centralized or distributed. These calculated trust values will be propagated in the network so that the trust can be established between nodes which are not in immediate contact. By propagating the trust, the trust values from multiple nodes will be collected from multiple nodes in order to make updated view of the trust. Here view means the kind of data structure used to store the parameters calculated like table etc. The updated view is preserved to act as history data in order to use fro future. The stored trust value can also be used in the trust calculation module in the form of feedback knowledge. Therefore trust calculation, trust propagation and trust updation modules are closely interconnected.

The detailed description of three layers used is given below:

A. Data Layer

Data collection module collects data based on behaviour of the nodes. Data is collected in the form of various parameters which are used to compute trust value. Various trust metrics are used to represent data.

1) Trust parameters:

This section introduces various parameters chosen to evaluate trust value.Li. X. et. al.[5] chose the following parameters to evaluate trust value: the number of successful and failed – route reply messages, route request acknowledgement packet, route error acknowledgement packets and data delivery acknowledgement packets.

Wenjia Li [13] used three parameters to evaluate trust value. These are packet drop rate(PDR), packet modification rate(PMOR), and packet misroute rate(PMIR) and can be defined as follows :

$$\text{PMIR} = \frac{\text{no. of packets misrouted}}{\text{total no. of packets}}$$

$$\text{PMOR} = \frac{\text{no. of packets modified}}{\text{total no. of packets}}$$

$$\text{PDR} = \frac{\text{no. of packets dropped}}{\text{total no. of packets}}$$

Virendera M. et. al. imlpied a node's trustworthiness by the following parameters: packet integrity, delay during forwarding, packet drops, insertion of duplicate or false packets, fake route information, generation of unnecessary control messages.

Y. Huang et. al.[16] defined the following statistics for a one hop neighbour to measure trust value: packets sent by the node but dropped by neighbour due to congestion or unknown reasons, packet forwarding delay at neighbour node, no. of packets misrouted, and packets falsely injected by the neighbouring node.

Yaser khamayseh et. al. [17] observes node's mobility, no. of neighbours each node has, number of packets generated and forwarded by the neighbouring nodes and the past activity of the node. Those parameters are then used to determine which nodes are misbehaving in the network.

Aakanksha Bedi [1] have used mobility and group behaviour properties of the node as measure for trust value of the node.

Shankaran R. et. al.[10] uses device capability in terms of hardware configuration, battery status, software configuration for deriving the trust value.

2) Trust metrics:

Trust is evaluated on different metrics and different ways. Some schemes use continuous and discrete values to measure the level of trust. For example, trust is described by a continuous value in (0,1) or measured as discrete value in (-1,1). Threshold based approaches are alsoused to measure the trust. Trust metrics such as fuzzy based, probability based, similarity, mobility, context based factors like energy , signal strength, hop distance etc.

B. Implementation Layer

This layer is responsible for calculating trust view then exchanging the view with the neighbouring nodes and corresponding updating the trust view. The updated view of the trust is further preserved as history data for evaluating the trust in future.

1) Trust calculation

There are two approaches used for calculating trust in MANETs. These are given below:

- Centralized trust approach
- Distributed trust approach

In centralized trust computation, a central trust manager computes trust value on behalf of all other nodes. In distributed architecture each node acts as a trust manager.

The centralized trust system calculates Global Trust Value (GTV) for every node.The centralized trust manager collects observations from nodes participating in the network and then these observations are combined together to calculate GTV. Centralized trust management system uses cooperation stimulation mechanisms. In these mechanisms, the trust value of a subject node is used by another nodes from the network to decide the strategy for interactions. If subject node's trust value is less than a threshold, then other nodes may isolate the node from network opertaions.

A Gossip based outlier detection algorithm is used in [15] in which outlier node is detected based upon their trustworthiness calculation. Every node exchanged their local view table with its neighbours until they have the same view generated which is called global view table which consists of trustworthiness value of each node. The trustworthiness is calculated as shown in figure 2.

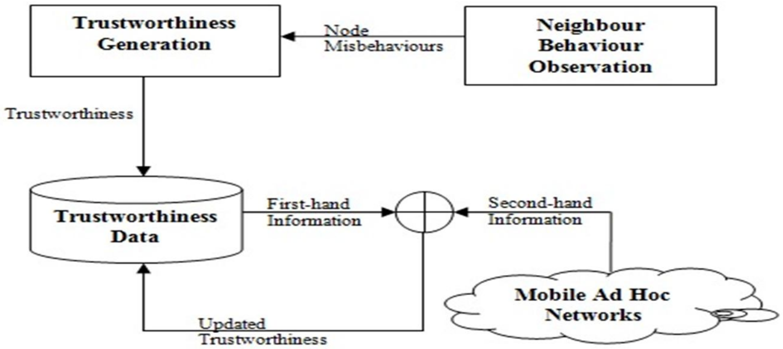

Figure 2: Trust Management Scheme

In Distributed trust calculation, trust levels are devised from the analysis of collected data from observations for specific actions. Trust levels can be classified as:

- Direct trust
- Indirect trust
- Hybrid trust

The **direct trust** is derived from node's own experiences about a particular node. Here trustor node directly observes behaviour of trustee node and is required for cases where a trust relationship is formed between two nodes without previous interactions. For example in [14] the trustworthiness Θ_k of a node N_k is defined as a function of all misbehaviours that other nodes have observed for the node $N_{k.}$ The trustworthiness is calculated as follows:

$$\Theta_k = 1- \sum P_i * M_{ki}$$

Here P_i denotes the punishment factor for the ith misbehaviour which indicates the severity degree of its outcome. M_{ki} represents the rate of this misbehaviour over the total observed behaviour. For example if packet drop, packet modification and packet misroute are the exact three misbehaviours to be observed then Θ_k can be derived as follows:

$$\Theta_k = 1 - P_{drop} * PDR – P_{modification} * PMOR - P_{misroute} * PMIR$$

The **indirect trust** is computed from recommendations given by other nodes about the trustee node. It may also receive this information second hand through the form of recommendations as in figure. If the past interactions are less or the behaviour of the nodes changes frequently, there will be scarcity of up to date information, in such type of scenario indirect trust is more useful.

A recommendation based trust [7] consists of the recommendation, R(b), defined as the weighted average of recommendations from all nodes $i \epsilon k_a$ about node b. The weight for a recommendation from a neighbour i is the trust level that node a has on node i, as follows:

$$R_a(b) = \frac{\sum_{i \in k_a} T_a(i) M_i(b) X_i(b)}{\sum_{j \in k_a} T_a(j) M_j(b)}$$

Here recommendations considers not only the trust level of other nodes(Ta), but also the accuracy(X_i) and the relationship maturity(M_i).

The hybrid trust is calculated by combining direct and indirect trust. A trust establishment strategy based on hybrid trust is presented in [9]**.** Here node n's trust on another node m is calculated as below:

$$T_{n,m} = \alpha 1 * nT^{m}S + \alpha 2 * nT^{m} O$$

Here $nT^{m}S$ is node n's direct trust on m which is calculated using direct monitoring of node m. The $nT^{m}O$ is indirect trust computed from other node's recommendations about node m. The α1 and α2 are weighting factors such that α1+α2=1.

2) Trust propagation

Trust calculation on a particular node by any other node incurs a cost on resources. These resources especially in MANETs are scarce. In order to reduce resources spent on re-evaluation of trust by other nodes can be reduced if the computed trust gets propagated in the network as shown in the figure[11] below. Trust propagation can be of multi hop. Trust propagation is based on transitivity property of the trust. The core factor to be considered for trust propagation is co-operation in the network in transporting the trust information.

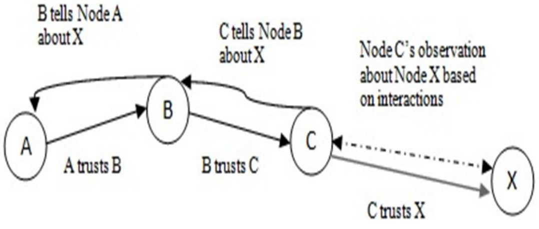

Figure 3: Trust propagation

3) Trust updation

There are various methods for updating the trust value by combining the evidences collected about different nodes such as simple mean, weight based method, probability based, fuzzy based, uncertainty based etc. Bayes theorem and Dempster Shafer theory(DST) are most suitable approaches for trust updations in MANETs. DST is more suitable when there is uncertainty or even no prior knowledge for the event take place. A trust updation method using dempster shafer theory (DST) of combination is presented in [2**].** Using DST, a node combines direct experience with indirect information(recommendation) ,the latter is first filtered based on data centric trust values acting as dynamic weighting factors. In DST evidence that does not support a given hypothesis is not considered as evidence for rejecting it. Belief in a hypothesis derives from a DSTprimitive called basic probability assignment(bpa). The total bpa supporting X is known as the belief function:

$$\boldsymbol{Bel(X) = \sum_{X' \subseteq X} m(X')}$$

and the total bpa that does not refute X is known as the plausibility function:

$$\boldsymbol{Pl(X) = \sum_{X' : X' \cap X \neq \emptyset} m(X')}$$

The functions Bel and Pl are interrelated in the obvious way.To combine pieces of evidences received from multiple sources , Dempster's combination rule uses the following associative operation:

$$\boldsymbol{m(X) = (m1 \oplus m2)(X) = \frac{\sum_{Y,Z : Y \cap Z = X} m1(Y) m2(Z)}{1 - C12}}$$

where m1 and m2 represents evidences received from two sources and C12 is the corresponding mass of conflict:

$$\boldsymbol{C12 = \sum_{Y,Z : Y \cap Z = \emptyset} m1(Y) m2(Z)}$$

C. Application Layer

Application of trust management is enormous in mobile networks. Cryptography is one of the most explored and widely deployed way of providing security services. Cryptography measures are often classified as hard security measures, which provide partial security solution by enabling data confidentiality, integrity, node authentication and non repudiation.

The category of threat which are purely due to node behaviours are classified as soft security. Soft security threats can be most effectively handled using trust management systems. Trust management cannot be seen as a complete replacement for cryptography, rather a supplement to it. Cryptography and trust management can work together to provide holistic security solution in MANETs.

V. CONCLUSION

In this paper, main characteristics of trust in MANETs are presented and a three layered trust based system design is proposed. Three layers contain data collection, trust calculation module and application module. Data collection module collects data by observing various trust parameters and represented in a trust metric and trust calculation module is responsible for computing trust value, trust propagation and trust updation.

Trustworthiness value used for the specific application purpose e.g. access control, misbehaviour detection etc.

REFERENCES

[1] AakankshaBedi: MPG-TAR: Mobile Process Groups Based Trust AwareRouting Protocol for MANETs, in International Conference on Advancesin Recent Technologies in Communication and Computing (ARTCom),vol., no., pp. 131-135, (2010).

[2] Jerzy Konorski and RafalOrlikowski,” Data-Centric Dempster-Shafer Theory-Based Selfishness Thwarting via Trust Evaluation in MANETs and WSNs”,IEEE,3rd international conference on new technologies, mobility and security,2009, pp 1-5.

[3] K Govindan and P. Mohapatra, “Trust computations and trust dynamics in mobile adhoc networks: A survey”IEEE Communication Surveys & Tutorials,2012, vol. 14, no. 2, pp. 279–298.

[4] K.SeshadriRamana, Dr. A.A. Chari, Prof. N.Kasiviswanth, “A Survey On Trust Management For MobileAd Hoc Networks”, International Journal of Network Security & Its Applications (IJNSA), Volume 2, Number 2, April2010,pp 75-85.

[5] Li X., Jia Z., Zhang P., Zhang, R., Wang H.: Trust-based on-demandmultipath routing in mobile adhoc networks, IET Information Security,vol.4, no.4, pp. 212-232, (December 2010).

[6] M. Deutch, “Cooperation and trust: Some theoretical notes,” Nebraska Symposium on Motivation, Nebraska UniversityPress, pp. 275–319, 1962.

[7] Pedro B. Velloso, Rafael P. Laufer, Daniel de O. Cunha, Otto Carlos M. B. Duarte, and Guy Pujolle, “Trust management in mobile ad hoc networks using a scalable maturity-based model”, IEEE Transactions on Network and Service Management, VOL. 7, NO. 3, 2010,pp 172-185.

[8] Ruidong Li, JieLi ,Peng Liu ,Hsiao-Hwa Chen, “An Objective Trust Management Framework for Mobile Ad Hoc Networks” IEEE 65th Vehicular Technology Conference, 2007,pp 56-60.

[9] Sandeep A. Thorat, P. J. Kulkarni,” Design Issues in Trust Based Routing for MANET”, IEEE, ICCCNT, 2014, pp 1-7.

[10] Shankaran, R., Varadharajan V., Orgun, M.A., Hitchens, M.: Context-Aware Trust Management for Peer-to-Peer Mobile Ad-Hoc Networks, in33rd Annual IEEE International Conference on Computer Software and Applications, vol.2, no., pp. 188-193,(2009).

[11] Vijayan R.,Jeyanthi N., “A Survey of Trust Management in Mobile Ad hoc Networks”, International Journal of Applied Engineering Research, Volume 11, Number 4 ,2016, pp 2833-2838.

[12] Virendra M., Jadliwala M., Chandrasekaran M., Upadhyaya S.: QuantifyingTrust in mobile ad-hoc networks, in International Conference onIntegration of Knowledge Intensive Multi-Agent Systems, pp. 65- 70,(April 2005).

[13] Wenjia Li and Anupam Joshi, “Outlier Detection in Ad Hoc Networks Using Dempster-Shafer Theory”, IEEE, Tenth International Conference on Mobile Data Management: Systems, Services and Middleware,2009, pp-112-121.

[14] Wenjia Li, Anupam Joshi and Tim Finin, “Coping With Node Misbehaviors In Ad-hoc Networks: A Multi-Dimensional Trust Management

[15] Wenjia Li, Anupam Joshi, Tim Finin, “CAST: Context-Aware Security And Trust Framework For Mobile Ad-hoc Networks Using Policies”, International Conference on Distributed Parallel Databases, Springer, New York 2013,pp 353-376.

[16] Y. Huang and W. Lee.: Cooperative Intrusion Detection System for adhocNetworks, in Proceedings of the ACM Workshop on Security of AdHocand Sensor Networks (SASN TM 03). Fairfax VA(October 2003).

[17] Yaserkhamayseh, Ruba Al-Salah, MuneerBaniYassein, “Malicious Nodes Detection in MANETs:Behavioral Analysis Approach”, Journal Of Networks, Vol. 7, No. 1, January 2012,Pp 116-125.