A Survey on Trust Models in MANET

[1]Juhi Kaneria, [2]Hiteishi Diwanji
[1]M.E.Scholar, [2]Associate Professor
Computer Science and Technology, LD College of Engineering, Ahmedabad
[1]kaneria.juhi@gmail.com, [2]hiteishi.diwanji@gmail.com

***Abstract*— Mobile Ad hoc network (MANET) consists of a set of mobile nodes in an inherently insecure environment, having limited battery capacities. Since MANET do not have a fix infrastructure, wireless links are vulnerable and topology changes randomly, securing MANET is difficult than the traditional networks. In ad-hoc network mobile nodes comes and leaves the network so providing trust in such a network is crucial task. In this paper we survey different properties of trust like context dependency, asymmetricity, transitivity, etc. and cluster based and maturity based trust schemes are presented. A cluster based trust evaluation schemes for MANET is presented to overcome the limited information about unacquainted nodes and to lessen the memory space. The proposed cluster-based trust model can quickly obtain the trust value even in the situation where there has been no experience data available. In this scheme the concept of inter cluster recommendation trust was introduced. The trust value was calculated using the reputation from a neighbouring node. In this model, a network was divided into clusters with one special node (cluster head) responsible for establishing trust relationship for internal clusters dynamically based on previous transactions result. The head node issues the certificate showing the trust level of each member node. When a node moves from one cluster to another, its trust level is determined by the certificate issued by previous cluster-head. This model can monitor the selfish behaviour of nodes in the network and isolate the selfish nodes from the network to enhance the effectiveness throughout the network. In maturity based scheme, trust is based on previous individual experiences and on the recommendations of others. Recommendation Exchange Protocol (REP) is used that allows nodes to exchange recommendations about their neighbors. This model does not require distribution of the trust information over the entire network. Without the need for a global trust knowledge, maturity based trust evaluation scheme rules well for large networks while still reducing the number of exchanged messages and therefore the energy consumption.**

***Keywords*—MANET, Trust, Trust evaluation, Cluster based trust model, Maturity based trust model**

I. INTRODUCTION

Mobile ad-hoc network (MANET) is an infrastructure less collection of mobile devices connected by wireless links. Nodes in MANET have an ability to move from one place to another and change its configuration dynamically. Each node functions as both a host and a router. Network topology is dynamic since the connectivity among the nodes varies with time due to node departures, new node arrivals and chances of having mobile nodes. Thus there is no fixed communication structure and no base station is present to organize communication pattern. MANETs allow nodes to move freely and wherever they require and group themselves using the wireless network topology i.e. 'on the fly' and may also be changed frequently without any predictions. MANET devices are connected with their respective nodes through direct wireless transmissions and too far away nodes through multi hop transmissions[1]. In multi hop transmissions, a node willing to transmit any data uses other nodes as medium for its transmissions. Hence a node in ad-hoc networks mainly depend on intermediate nodes that serve in providing routes and forward packets to the targeted node. Also, node provides the advantages like flexibility, robustness and mobility support. In spite of such advantageous features there arise new challenges and issues regarding security.

MANETs are usually more prone to physical security threats. The possibility of eavesdropping, spoofing, denial-of- service, and impersonation attacks increases [2]. Similar to fixed networks, security of the ad hoc networks is considered from the attributes such as availability, confidentiality, integrity, authentication, non-repudiation, access control and usage control [3, 4].

Security approaches used for the fixed networks are not suitable for ad-hoc networks due to their salient characteristics. Thus there is a need to build new security mechanisms to adapt to these special characteristics of MANET.

Trust is an important aspect in the design and analysis of secure distribution systems [5]. It is also one of the most important concepts guiding decision-making [6]. Trust is a critical part of the process by which relationships develop [7]. By clarifying the trust relationship it will be easy to take proper security measures and make appropriate decision on any security issues. Trust establishment is a challenging and an important issue in the security of ad hoc networks. The lack of infrastructure in MANET makes it difficult to ensure the reliability of packet delivery over multi-hop routes in the presence of intermediate malicious nodes. A trust model specifies, evaluates and sets up trust relationship among entities.

To adapt to particular characteristics and defend against new threats, new security schemes based on trust evaluation are proposed [2]-[5]. In these schemes, each node evaluates the trust of the other nodes with which it communicates. The evaluation for the other node is performed by evaluating the node's own experience about the evaluated node. Based on the evaluated trust, security measures are taken, or security decisions are made.

In this paper, in section II and section III, we present the concepts of trust and its properties. In Section VI trust evaluation scheme is surveyed. Finally the conclusion and directions of future work are given in last section.

II. CONCEPT OF TRUST

Trust is a concept hard to define because it is itself a subjective term. There are several definitions of trust.

Two definitions of trust are given. Gambetta defined the "Evaluation Trust" as the subjective probability by which an individual, A, expects that another individual, B, performs a given action on which its welfare depends. McKnight & Chervany defined the "Decision Trust" as the willingness to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible. Trust is dependent on the reputation of the system.

Josang defines aspects of trust that include trust scope, functional trust, referral trust, direct trust and indirect trust. Trust scope "σ" is a function that the relying party depends on and trusts. The trusted party performs the function in case of Functional trust "fσ". In case of Referral trust "rσ", the trusted party recommends a party that can perform the function. Direct trust "dσ" is the result of direct experience. Indirect trust "iσ" is derived from recommendations. Trust measure μ can be defined as Binary (Trusted, not trusted), Discrete(strong, weak, trust, distrust), Continuous(percentage, probability, belief). Time τ is a time stamp when trust was assessed and expressed. This is needed as trust is built with time and also decreases with time.

III. PROPERTIES OF TRUST

The trust metric itself has the following properties.

- Context dependence: The trust relationships are only meaningful in the specific contexts.
- Function of uncertainty: Trust is an evaluation of probability of if an entity will perform the action.
- Quantitative values: Trust can be represented by numeric either continuous or discrete values.
- Asymmetric: Trust is not necessarily symmetric, meaning not identical in both directions. That is, if A trusts B, it is unnecessary to hold that B trusts A.
- Transitive: Trust is transitive, i.e., if node A trusts node B and node B trusts node C, then node A trusts node C. But in reality trust is not perfectly transitive in a mathematical sense. That is, if A trusts B, and B trusts C, it does not guarantee that A trusts C.
- Personalized: Trust is inherently a personal opinion. Two people often evaluate trustworthiness about the same entity differently.

IV. TRUST MODEL SCHEMES

A. CLUSTER BASED TRUST MODEL

In [12] Cluster based trust model for MANET was introduced. Cluster based model aims at maintaining dynamic and efficient trust relationship in MANET. Cluster based trust evaluation scheme was proposed to overcome the limited information about unfamiliar nodes and to reduce the memory space. In this model, ad-hoc network divided into clusters as shown in "Figure 1". In this model, neighboring nodes form a cluster and evaluates its neighbor nodes trust values based on its experience. Each node then selects one node with highest value as a trust guarantor which becomes the cluster head and the chooser becomes a member of the cluster. If the chosen node is already a member of another cluster, a node of the second highest trust value is chosen. The head issues a trust value certificate that can be referred to by its non-neighbor nodes. In this way, an evaluation of an unfamiliar node's trust can be done very efficiently and precisely [13].

1) Direct trust Representation & its computation [14, 15, 16]

Direct trust is the probability which node N_i calculates that N_j behaves positively to perform the requested action. Node N_i takes into account the individual experiences of the past transactions with N_j. No recommended experiences but only new individual experiences may lead to new direct trust value. If N_i and N_j have t is times transactions with t_m times success and a is a positive real number such that a is inversely proportional to evidence in this model, then direct trust is represented as TR_D^{ij} and is calculated as under:

$$TR_D^{ij} = \frac{t_m + a/2}{t + a} \quad t_m, t \geq 0, a > 0$$

If there is no previous interaction between N_i and N_j($t=t_m=0$) then direct trust value is 0.5 which serves as encourage mechanism for new nodes. If the first interaction is success, the direct trust value increases rapidly and on contrary, its decreases rapidly. In MANET there is no absolute trust or distrust so $0< TR_D^{ij} <1$.

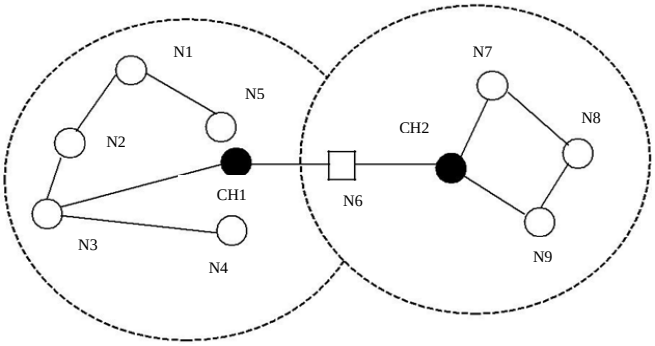

Figure 1 Cluster based trust model in MANET

2) Intercluster Recommendation Trust value's Representation & its calculation[17]

In MANET nodes enter and leave the network frequently. So measuring trust of other nodes to new nodes is challenging. Recommendation trust is used to help establish trust relationships between unknown or unfamiliar nodes. However, because recommendations have uncertainty or risk, nodes need to know how to cope with second-hand information [10]. To solve this problem, inter-cluster recommendation trust is presented. CH calculates the recommendation trust for every cluster members in the cluster. The recommendation information is the direct trust value of each node to the single node and this scheme takes the direct trust of each node to CH as the recommendation's weight. Furthermore, in order to save bandwidth, CH discards their recommended value, if the node's direct trust by CH lowers than a threshold value H. The value of H is decided by the local policy of CH. The inter-cluster recommendation trust metric for N_j is:

Intercluster recommendation trust value is represented as TR_r^j and calculated as:

$$TR_r^j = \frac{\sum_{i=1}^{t} TR_D^{hi} . TR_D^{ij}}{\sum_{i=1}^{t} TR_D^{hi}}$$

TR_D^{hi} is aggregation weight i.e. direct trust value of node Ni computed by CH, TR_D^{ij} is direct trust recommendations information and n is the number of nodes in current cluster.

3) Total trust representation & computation[17]

Total trust is given by Γ(Ni, Nj) and calculated as :

$$\Gamma(N_i, N_j) = \alpha TR_D^{ij} + \beta TR_D^{i}$$

where α, β ≥ 0 and α + β = 1. TR_D^{ij} is the direct trust between nodes N_i and N_j, α is the impact weight of direct trust and β is the impact weight of recommendation trust.

4) Cross cluster trust[17]

The cross cluster trust between nodes N3 & N7 can be calculated as:

$$\Gamma(N_3, N_7) = \Gamma(N_3, N_6) + \Gamma(N_6, N_7)$$

Nodes N_3 and N_7 are in cluster C_1 and C_2 respectively and both are connected through node N6 (gateway). (N_3, N_6) is the global trust of node N_6 by node N_3.This trust value is calculated in c1 because node N3 and N6 locates in c1. (N_6, N_7) is global trust, which calculates in cluster c_2 because node N_6 and N_7 comes in cluster c_2.

B. MATURITY BASED TRUST MODEL

In maturity based trust model, every node is having the trust values of their specific neighbour in MANET which gives view of the behaviour history of those nodes. Trust values will be calculated as the combination of past experiences and on the opinion of the node's neighbour. Every node takes direct recommendation value to its neighbourhood node only. This value will be decreased if new neighbour comes in network. Recommendations can speed up the convergence of the trust evaluating process. It introduces the concept of relationship maturity in Ad-hoc network i.e. trust increases between people as times goes by, same concept is used in maturity based model for MANET. This concept allows nodes to give more importance to recommendations send by long-term neighbours rather than short-term neighbours. This model proposed the REP (Recommendation Exchange Protocol) for interchanging recommendation value for their neighbours.[17]

1) Calculation of recommendation value in Ad-hoc

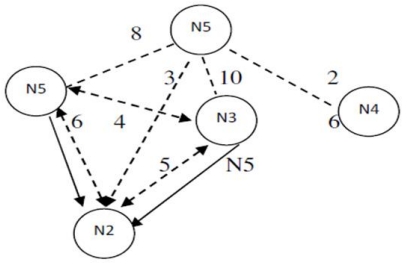

Figure 2 Evaluation of recommended trust

In "Figure 2", decimal digits show how long the nodes know each other. Dotted arrows are used for connecting the neighboring nodes. Normal arrow indicates recommendation. Here N_5 is neighboring node of N_2, N_1 & N_3. Nodes N_1 and N_3 send recommendation value of N_5 to N_2. N_2 consider the recommendation value (5) of N_3 more important than N_1 because node N_3 knows node N_5 as longer period of time also N_3 having more older experience to interact with N_5 as compared to N_1.

2) Maturity based trust model operation modes

The three types of operation modes for maturity based trust model are: Simple Mode, in which node using trust table and REP protocol optional. Nodes operated in less power capacity. In Intermediate Mode, nodes are operated in medium capacity and takes recommendations of other nodes. Advanced Mode, nodes are operated in higher power capacity & developed the system with all features. REP protocol is used for providing interface between network (TCP/IP) and trust, learning plan of System.

3) Evaluation of Trust in Maturity based Model

The evaluation of trust from node a to b is denoted as Ta (b).$T_a(b) = (1-\alpha)Q_a(b) + \alpha R_a(b)$ where α ranges from 0 to 1, $Q_a(b)$ presents direct trust and lies between 0 to 1 and from [22] the aggregate recommendation value of all other neighbors is denoted by $R_a(b)$and is calculated as

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

4) Working of REP Protocol

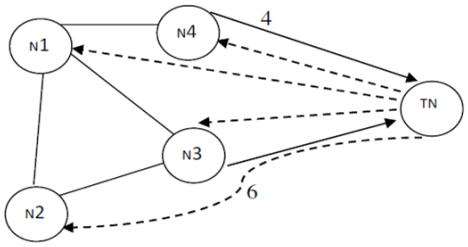

Figure 3 Working of REP Protocol

This protocol permits the nodes to interchange recommendations value between neighboring nodes. REP uses 3 messages, Trust request (TREQ), Trust reply (TREP) and Trust advertisement (TA). REP works as follows:

When new nodes (TN) come in network it sends TREQ message with IP address to each node (⇢)

Now neighboring node will only sends TREP with its recommendation value to TN (target node) (→)

V. CRITICAL ANALYSIS

In cluster based trust model zone routing protocol is used and for trust calculation mathematical equations are used. There is no need of personal or past experience for evaluation of trust values in MANET. Effective work in a small scale Ad-hoc network, Cluster head (CH) and gateways used in this model. There is no need of centralized infrastructure. Whereas in maturity based trust model, trust increases with the passage of time. This scheme doesn't need authentication mechanism. Nodes do not need to know nor recognize any other node a priori, namely, a node does not to identify a new neighbor when it arrives. In this system, nodes must be able to identify neighbors that they already know. Therefore, there is no need of a certification authority. Hence, nodes must exchange identifiers when they first meet and keep a neighbor identifier during all the period they remain in the radio range of each other. There is low vulnerability to false recommendation attack. It requires less resource consumption. This model is robust to slander colluding attack. Any change in behavior of node can be easily identified by this model. It can be applied to both small and large scale ad-hoc networks.

VI. CONCLUSION

In this paper, concepts of trust along with its several properties like context dependency, asymmetricity, transitivity, etc.

were presented. Also comparative survey of cluster based and maturity based trust models for mobile ad-hoc network to achieve the security and trustworthiness was carried out. A cluster based trust evaluation schemes studies here overcomes the limited information about unfamiliar nodes and reduces the memory space. This model monitored the selfish behavior of nodes in the network and isolated the selfish nodes from the network to enhance the effectiveness throughout the network. In maturity based scheme, trust is based on previous individual experiences and on the recommendations of others. Recommendation Exchange Protocol (REP) is presented that allows nodes to exchange recommendations about their neighbors. In maturity based model, the interactions among nodes are confined to neighbors. Such approach implies lower resource consumption and a lower vulnerability to false recommendations attack. Another important quality is the flexibility due to the possibility of operating in three different modes, depending on the node resource restrictions. Thus, our model is suitable for heterogeneous network, where nodes present distinct constraints. Thus, maturity based model is better as compared to cluster based trust evaluation scheme. In future work, these schemes can be integrated to obtain effective trust evaluation.

REFERENCES

[1] D. Ganesh and M. Sirisha, "Reputation and Trust Evaluation in MANETs Using Eigen Trust Algorithm" in VSRD-IJCSIT, Vol. 2 (3), 2012.

[2] S. Corson, J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations" inIETF RFC2501, 1999.

[3] L. Zhou, Z. J. Haas, "Securing Ad Hoc Networks" in IEEE Network, 13(6): 24-30, Nov/Dec 1999.

[4] Yongguang Zhang, Wenke Lee, "Intrusion Detection in Wireless Ad-Hoc Networks" in Proceedings of MobiCom 2000, Sixth Annual International Conference on Mobile Computing and Networking, Boston, MA, USA, 6-11 Aug. 2000.

[5] Diamadi, Z. Fischer, M.J, "A simple game for the study of trust in distributed systems" in International Software Engineering Symposium 2001 (ISES'01), Wuhan University Journal of Natural Sciences Conference. March 2001.

[6] Shillo, M.; Funk, P.; Rovatsos, M, "Using trust for detecting deceitful agents in artificial societies" in Applied Artificial Intelligence, vol.14, no.8, p.825-48 Sept. 2000.

[7] Warne, D., Holland, C.P, "Exploring trust in flexible working using a new model" in BT Technology Journal, vol.17, no.1, p.111-19. Jan 1999.

[8] Gambetta, "Can Trust:We MakingTrustand BreakingTrust?"Cooperative Relations, Basil Blackwell, Oxford, 1990, pp. 213-237.

[9] H. S. James, "The Trust Paradox: A Survey of Trustworthiness,"JournalofEconomicBehavior and Organization, vol. 47, no. 3, 2002.

[10] CHEN Aiguo, XU Guoai, YANG Yixian, "A Cluster-Based Trust Model for Mobile Ad hoc Networks",IEEE 2008.

[11] D. McKnight and N. Chevany, "The Meanings of Tru of Minnesota, Technical Report TR 94-04, 1996.

[12] CHEN Aiguo, XU Guoai, Yang Yixian, "A Cluster Based Trust Model For Mobile Ad-hoc Networks", 2008 IEEE.

[13] Seunghun Jin, Chanil Park, Daeseon Choi, Kyoil Chung, and Hyunsoo Yoon "Cluster-Based Trust Evaluation Scheme in an Ad Hoc Network" in ETRI Journal Volume 27, Number 4, August 2005

[14] CHEN Aiguo, XU Guoai, Yang Yixian, "A Cluster Based Trust Model For Mobile Ad-hoc Networks", 2008 IEEE.

[15] R.Cramp, "Logical foundations of probability", University of Chicago press, 1950.

[16] R.Cramp, "Replies and systematic expositions", in P.A. Schilpp (ed.), the philosophy of Rudolf Carnap. La Salle, Illinois, Illinois: Open court, 1963, pp. 966-998.

[17] Renu Dalal, Manju Khari and Yudhvir Singh, "Different Ways to Achieve Trust in MANET" in International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 2, April 2012

[18] N. Saxena, G Tsudik, and J.H. Yi, "Threshold Cryptography in P2P and MANETs: the case of access control, "Computer Networks, Vol. 51, No.12, pp.3632-3649, 2007.

[19] B. Wu, J. Wu, E.B. Fernadez, M. Ilyas, and S. Magliveras, "Secure and efficient key management in Mobile ad hoc networks," Journal of Network Computer Applications, Vol.30, no.3, pp. 937-954, 2007.

[20] D. Joshi, K. Namuduri, and R. Pendse, "Secure, redundant, and fully distributed ket management scheme in mobile and ad-hoc networks: an analysis," EURASIP journal on wireless Communications and networking, Vol. 2005, no. 4, pp.579-589, 2005.

[21] S.Capkun, L Buttyan, and J.P Hubaux, "Self-organized public key management for mobile ad-hoc networks," Mobile Computing and Communication Review, vol.6, no. 4, 2002.

[22] P. Caballero-Gill and C. Herandez-Goya, "Efficient Public Key Certificate Management for Mobile Ad-hoc Networks," EURASIP journal on wireless Communications and networking, vol. 2011, pp.1-10, 2010.