International Journal of Computer Systems (ISSN: 2394-1065), Volume 02– Issue 05, May, 2015
Available at http://www.ijcsonline.com/

Vector Trust Aggregation Management Model for Secure Routing in Mobile Adhoc Networks

Jayalakshmi V [Á], Dr. Abdul Razak T [Ḃ]

[Á] Research and Development Center, Bharathiyar University, Coimbatore, India, jayasekar1996@yahoo.co.in
[Ḃ] Department of Computer Science, Jamal Mohamed College, Tiruchirappalli, India, abdul1964@yahoo.com

Abstract

MANET is a set of limited range wireless nodes that function in a cooperative manner so as to increase the overall range of the network. The performance of ad hoc networks depends on the cooperative and trust nature of the distributed nodes. To enhance security in ad hoc networks, it is important to evaluate the trustworthiness of other nodes without centralized authorities. In this paper, a novel dynamic vector trust aggregation management model with multiple decision factors and vector trust aggregation is proposed. The multiple decision factors include weighted packet forwarding factor, similarity factor and time aging factor. These trust factors are incorporated to reflect trust relationship's complexity and uncertainty. Based on the trust factors, the selection of the trusted nodes with most trustable path is obtained by using Trust vector Aggregation. The trusted path obtained by using the proposed model eradicates malicious nodes and helps to protect the network from any internal attacks.

Keywords: *Adhoc networks, Attacks, Malicious nodes, security, Trust.*

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are collections of wireless mobile nodes, constructed dynamically without the use of any existing network infrastructure or centralized administration. Due to the limited transmission range of wireless network interfaces, multiple hops may be needed for one node to exchange data with another one across the network. MANETs are characterized by limited power resource, high mobility and limited bandwidth. Owing to the openness in network topology, the security of communication in ad hoc wireless networks is important, especially in military applications. The absence of central coordination mechanism and shared wireless medium makes MANETs more vulnerable to digital/cyber-attacks[1] than wired networks. These attacks are generally classified into two types: passive and active attacks. Passive attacks do not influence the functionality of a connection. An adversary aims to interfere in a network and read the transmitted information without changing it. If it is also possible for the adversary to interpret the captured data, the requirement of confidentiality is violated. It's difficult to recognize passive attacks because under such attacks the network operates normally. In general, encryption is used to combat such attacks. Active attacks aim to change or destroy the data of a transmission or attempt to influence the normal functioning of the network. Active attacks when performed from foreign networks are referred to as external attacks. If nodes from within the adhoc network are involved, the attacks are referred to as internal attacks.

In order to combat passive and active attacks, a secure ad hoc network is expected to meet the different security requirements such as Confidentiality, Integrity, availability, authentication and non-repudiation. Recently, there are many scholars contributing to the researches [2-5] on secure and trusted routing. They can be mainly classified into two categories: cryptographic technique and non-cryptographic technique. The cryptographic technique mainly focuses on traditional safety mechanisms called hard security strategy. These traditional safety mechanisms for providing confidentiality, authentication, and availability are not efficient in MANETs, where network nodes have limited communication bandwidth, CPU cycles, memory, and battery capacity. These traditional safety mechanisms come at the cost of computation complexity of encryption algorithms, memory usage for storing security information, and network bandwidth for key synchronization and certificate distribution and revocation.

In fact, the very challenge of securing distributed networks comes from the distributed nature of these network and the wireless nodes must cooperate in order to establish communications dynamically using limited network management and administration. Collaboration is only productive if all participants operate in an honest manner. Therefore, establishing and quantifying trust, which is the driving force for collaboration, is very important for securing distributed networks. Some trust models have been proposed in the wired networks. However, they are inapplicable to the MANET due to the difference in network topology and application scenario.

In this paper, a novel trust management model is proposed to select the trusted nodes which exclude the malicious nodes in order to establish a secure communication. The multiple trust decision [7, 8] evaluating factors are obtained and it includes weighted

packet forwarding factor, similarity factor and Time aging factor. Based on the trust decision factors, the trust value is calculated by assigning weight to each factor .The calculated trust value is propagated by using vector trust and the most trusted path is obtained by using the vector trust aggregation [9]. The path obtained by this model can kick out the untrusted nodes and helps to protect the network from any internal attacks.

The remaining paper is organized as follows. Section 2 describes the related work which gives the basic definition and metrics used in the trust and also the various trust management models proposed in the literature. In section 3 the proposed trust model is presented and it describes the various trust evaluating factors. Section 4 describes the vector trust and vector trust aggregation method to obtain the most trustable path and the conclusion is presented in the section 5.

II. Related Work

A standard definition considers trust to be a measure of subjective belief that one person or party uses to assess the probability another will perform a favourable action before the opportunity presents itself to monitor whether that activity has occurred. When a person is considered trustworthy; it is meant that there is a high probability that the actions they are expected to perform will be done in a manner that is favorable to the truster .The overall measure of trust that changes through time. The measurement of the trust [10] can be levied against the measure of risk and the measure of trust may also be affected by control systems in place.

A. Trust Models

Although there has been substantial work on trust management models, their applicability in mobile agent systems has received limited research attention

Beth et al. [11] proposed a trust management model, which introduced the concept of experience to express and measure trust, in which the credibility formula was derived and integrated. This model divided „trust" into direct trust and recommendation trust which were used to describe the trust relationship, respectively, between the subject and object, subject and recommendation object. A trust management model was proposed by Josang [12] based on the subjective logic model, which introduced the evidence space and the conception space to describe and measure the concept of trust relationships. This model defined a set of subjective logic operators for the derivation and comprehensive calculation of trust value. From the evolutionism and sociology points of view, Mui [13] first introduced a trust and reputation computing model for generalized networks. In the indirect trust evaluation process, they proposed a graph parallelization algorithm, which is intuitive and easy to understand. In the model established by Sun et al. [14, 15], trust is measured by entropy. They introduced an entropy function to represent the trust value between two nodes, which really captured the dynamic nature of trust evidence. To compute the indirect trust value, both George and Sun"s models used trust value iteration techniques considering multi-level directed graph. When more nodes are involved, the convergence speed of this scheme is exponentially slow, and its flexibility becomes a big challenge. In the subjective trust evaluation model proposed in the [16] uses the credibility of nodes can be evaluated using analytic hierarchy process theory and fuzzy logic rules prediction method. The model can detect malicious nodes only if there are few in the numbers and also it utilized AHP [17] to set up a hierarchical skeleton within which multi-attribute decision problems can be structured to determine the weight for the trust factors.

In the proposed trust management models in the literature, weight is not assigned based on the importance of the file and also the vector trust is used to obtain the most trusted route.

III. Trust Model

Definition : Adhoc network contains many nodes and these nodes are independent in nature and the network can be considered as a weighted graph $G = (V, E, Tv)$, where V is the set of all nodes, E is the set of all edges and $Tv:Tv(E_{ij}) \rightarrow R\varepsilon[0,1]$ denotes the value of the trust of the node. There is an edge between two nodes if they are located within each other"s transmission range. A path between the source node V_S and the destination node V_D can be represented as a node sequence $P = (V_S, \ldots V_i, \ldots, V_D)$, *where* $V_i \in V$.

The trust model of an adhoc network can be represented as the weighted directed graph as in the Fig.1. Each node in the model maintains a trust table which contains the trust values of the neighbouring nodes.

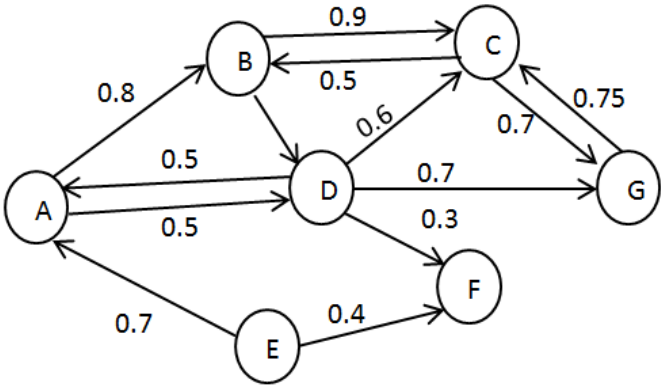

Fig 1. Weighted graph in the Adhoc Networks

In most existing trust models, direct trust [18] is based on the two neighbour entities historical interactions. In this paper, the trust value is calculated by averaging the weighted forwarding ratio and the similarity factor between the neighboring nodes which forwards packets.

A. Weighted Packet Forwarding Ratio

The ratio of number of packets forwarded correctly to the total number of packets is known as Forwarding Ratio (FR) [19].The packet forwarding ratio at time t is calculated as follows

$$FR(t) = \frac{N_{cor}(t)}{N_{all}(t)} \text{--------(1)}$$

Our proposed model, calculates the trust value with multiple constraints: weight factor assigned to each packet transmitted and time aging factor. Trust normally fades with time variation. A weight is assigned to each data being forwarded because some malicious nodes may forward data packets if they are of less importance and do not forward data packets of high importance. Based on the above constrains the packet forwarding ratio is modified to compute the trust value. The weighted packet forwarding ratio at time t is given in the equation (2)

$$FR_{(t)} = \frac{\sum_{j=1}^{n} \delta_j}{\sum_{i=1}^{m} \delta_i} \text{--------(2)}$$

δ is the weightage factor for the data based on its importance as shown below in the table 1. *n* is the number of packets correctly forwarded and *m* is the total number of packets forwarded.

TABLE 1. WEIGHTAGE OF PACKETS FORWARDED

S.No.	Importance	Value
1.	Important/Rare	>=0.8
2.	Control packets/ Medium	>=0.4 to <0.8
3.	Unwanted	<0.4

The trust information is given by the trust record list which contains monitored node ID, node"s trust value, two integer counters of i and j for the number of packets forwarded and the number of packets correctly forwarded without any modifications by the malicious nodes, a packet buffer and weight factor for packet forwarded. It is computed using forwarding count of all packets including the control packets and data packets according to the time t, the trust value of node v_j evaluated by node v_i is calculated by this equation (2).

B. Similarity Factor

Similarity [20] in MANET is a subjective judgment a mobile node makes about another"s owned attributes based on its preference and standpoint. Similarity indicates the relationship between user attributes. The mobile nodes having an exactly the same or similar affiliated organization may also have a stronger trust in each other than the ones with different affiliated organizations. Since trust is defined in the context of similarity conditions, the more similar the two users are the greater their established trust would be considered [21]. In order to compute the similarity between users, a variety of similarity measures have been proposed, such as Pearson correlation, cosine vector similarity, Spearman correlation, entropy-based uncertainty and mean-square difference. However, Breese et al in [22] and Herlocker et al. in [23] suggest that Pearson [24] correlation performs better than all the rest.

The notation V_i (a_1, a_2… an) denotes node V_i with n attributes (a_1, a_2,….,a_n). For two nodes V_i and V_j both with n attributes ($V_i(a_1, a_2,….,a_n)$, $V_i(a_1, a_2,….,a_n)$), the corresponding attributes have a certain similarity. One node can have more than one attribute, and these attributes have different numerical ranges. Some are composed of discrete variables, such as velocity and transmission range, where as some are depicted by linguistic description, such as moving direction and affiliated organization. The first step is to assign a unique value to different elements of a given attribute, e.g., the attribute value of velocity is given by its practical value. The established similarity trust between two nodes is defined as the Pearson Correlation [24] given in the equation.

$$ST_{(v_i,v_j)} = \frac{\sum_{k=1}^{n} (V_{i_{a_k}} - \bar{V}_{i_{a_k}})(V_{j_{a_k}} - \bar{V}_{j_{a_k}})}{\sqrt{\sum_{k=1}^{n} (V_{i_{a_k}} - V_{i_{a_k}})^2} \sqrt{\sum_{k=1}^{n} ((V_{j_{a_k}} - V_{j_{a_k}})^2}} \text{---(3)}$$

The Trust value of a node is calculated as follows,

$$TV(t) = \frac{\alpha FR + \beta ST}{2} \text{----------(4)}$$

α and β are the weights for the calculated forwarding ratio and the similarity Trust respectively. The values of α and β are chosen in such a way that $\alpha + \beta = 1$, $0 < \alpha < 1$ and $0 < \beta < 1$.

C. Time Aging Factor

The attenuation rate made by the kth interaction interval compares to the latest interaction interval in the trust computation is defined as the time aging function. Δt is the time interval between the trust calculation and it is 30 s.

$$AF = \frac{f}{(f+1)} \text{--------(5)}$$

$$f = \rho^{n-k}, 0 < \rho < 1, 1 \le k \le n \text{-----(6)}$$

The base coefficient ρ represents the attenuation factor. smaller ρ causes a greater attenuation of *f* and vice versa.

Finally, the node V_i computes node V_j"s trust according to history of interactions via the following equation:

$$TV_{ij}(t) = AFXTV_{ij}(k) \text{------(7)}$$

IV. VECTOR TRUST AGGREGATION METHOD

To propagate the calculated trust information in the network efficiently and accurately, we define the

concept of trust vector, trust transfer and most trustable path. This trust aggregation algorithm is designed to find the most trustable path in the network from source to destination.

A. Trust vector

An edge directed from node A to node B if and only if node B is a neighbour node to node A and can do direct transaction/interaction and A has a direct trust rating towards B. The value of the directed edge A to B reflects how much A trusts B .$T_{A,B}$ = 1 indicates A 100% trusts B , $T_{A,B}$ = 0 indicates A never trust B.

Definition: In Vector Trust, a personalized trust is propagated as a vector of trust rating and direction, where trust rating is defined as a real number T, T∈ [0,1] and direction is defined as a directed edge in the trust graph. This directed link with trust rating is called Trust Vector (TV).

If node A has a trust rating 0.8 on B , the trust vector is $T_{A,B}$ = 0.8 as shown in Fig.2

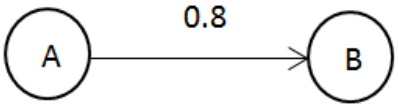

Fig 2. Vector Trust

Suppose A wishes to find a trust value for C. If A and C had prior transactions, then A can just look up the value of edge $A \rightarrow C$. However, if A and C have never had a prior transaction, A has to infer a trust value for C by using trust transfer.

B. Trust Transfer :

If node V_i has a trust rating $TV_{i,j}$ towards node j, node j has trust rating $TV_{j,k}$ towards node k, then node i has indirect trust $TV_{i,k} = TV_{i,j} \times TV_{j,k}$ towards node k.

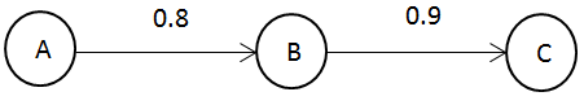

Fig 3. Trust Transfer

As shown by Fig. 3, A has indirect trust $T_{A,C}$ toward. C. $T_{A,C} = T_{A,B} \times T_{B,C} = 0.8 \times 0.9 = 0.72$.

C. Most Trustable Path

There might be many trust paths from node A to node C. Given a set of paths between A and C, A tends to choose the *Most Trustable Path* (MTP) to finish multihop transactions with an unfamiliar node C.

The most trustable path from node i to node k is the trust path yielding highest trust rating $TV_{i,k}$.

In Vector Trust, the most trustable path can be computed as the maximal product value of all directed edges along a path. And this product will be considered as A's trust rating towards C. In the example shown in Fig.4, the MTP is

$A \rightarrow B \rightarrow C$, and A infers a trust rating of $T_{A,C} = 0.72$ toward C.

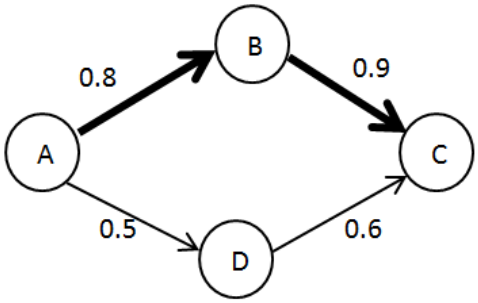

Fig 4. Most Trustable Path

For each direct transaction in the system, participating nodes generates a direct trust link and assigns a trust rating based on the calculations used in the section 3 to represent the quality of this transaction. For example, consider a successful transaction between nodes A and B in which A is the neighbor of B. After the transaction completes, node A assigns a trust rating to reflect the quality of B's service. And a new link starts from A with the arrow point to the server B will be added in trust graph. A stores this rating in its trust table.

The trust table is required for each node. It consist of the destination nodes address as entry, the trust rating, the next hop and the total hops (optional) to reach the destination. Each entry shows only the next hop instead of the whole trust path.

D. Trust Vector Aggregation

In the initial stage of the transmissions in the network, direct trust values calculated by using methods given in the previous section and values are stored in local trust tables. However, the direct trust information is limited and does not cover all potential interactions. For most nodes without adequate direct trust information, they have to use indirect trusts to start the process. An algorithm for *Trust Vector Aggregation* (TVA) is proposed to infer and aggregate trust values. In this algorithm, each trust path is aggregated to MTP with most reliable trust rating towards a target node by the value iteration process. Indirect trust information will be added to a trust table and be updated as the aggregation process evolves. Note that, trust aggregation does not create any new link in the network. Links are created or modified only after direct transactions.

Where $TV_{i,k}$ is the trust rating towards node k given peer i's local trust table, $TV_{i,j}$ is the direct link trust and $TV_{i,k}$ is the received trust information towards node k.

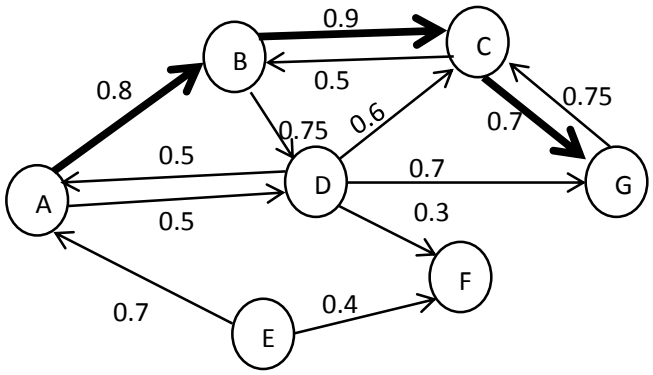

Fig. 5. An example network with 7 nodes

As an example, consider above network in fig. 5 with 7 nodes, A is the source node and G is the destination node. There are 4 paths exists from souce node to destination in the fig.5.

Path 1 = A→B→C→G, the computed trust rating for this path is 0.504 (0.8 X 0.9 X 0.7)

Path 2 = A→D→G has trust path rating of 0.35 (0.5 X 0.7)

Path 3 = A→B→D→G has the trust path rating of 0.42. (0.8 X 0.75 X 0.7)

Path 4 = A→B→D→C→G gives the path rating of 0.252 (0.8 X 0.75 X0.6 X 0.7)

Considering the all the four paths, the path with more trust rating i.e. path 1 A→B→C→G is chosen as the most trustable path to transmit packets to the destination. The route obtained by the vector trust aggregation method gives the with the minimum hop counts. When the number of hops is more, the vector trust aggregation will give the less trust value and that path is not chosen for transmission.

V. CONCLUSION

In this paper, a novel trust management model has been proposed based on the trust vector aggregation method. The multiple trust factors are used to calculate the accurate trust value. The novel trust model presented in this paper can kick out the untrustworthy nodes and selects the most trustable path with minimum hop counts so that a reliable passage delivery route is obtained. To make further improvement for the trust model proposed in this paper, we plan to incorporate other decision factors to our trust model. In addition, as an application of the proposed trust model , a novel reactive routing protocol on the basis of the standard dynamic source routing, a new trusted dynamic source routing protocol will be proposed and the comprehensive performance evaluation will be conducted to compare with other routing protocols.

REFERENCES

[1] Kannhavong, Bounpadith, et al. "A survey of routing attacks in mobile ad hoc networks." Wireless communications, IEEE 14.5 (2007): 85-91.

[2] Y-C Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," IEEE Sec. and Privacy, May–June 2004.

[3] K. Sanzgiri et al., "A Secure Routing Protocol for Ad Hoc Networks," Proc. 2002 IEEE Int'l. Conf. Network Protocols, Nov. 2002

[4] Li, Xiaoqi, Michael R. Lyu, and Jiangchuan Liu. "A trust model based routing protocol for secure ad hoc networks." Aerospace Conference, 2004. Proceedings. 2004 IEEE. Vol. 2. IEEE, 2004.

[5] Ghosh, Tirthankar, Niki Pissinou, and Kami Makki. "Towards designing a trusted routing solution in mobile ad hoc networks." Mobile Networks and Applications 10.6 (2005): 985-995.

[6] Pirzada, Asad Amir, and Chris McDonald. "Trust establishment in pure ad-hoc networks." Wireless Personal Communications 37.1-2 (2006): 139-168.

[7] Xiao-Lin, LI Xiao-Yong GUI. "Trust Quantitative Model with Multiple Decision Factors in Trusted Network [J]." Chinese Journal of Computers 3 (2009): 004.

[8] Xia, Hui, et al. "A Subjective Trust Management Model with Multiple Decision Factors for MANET Based on AHP and Fuzzy Logic Rules." Proceedings of the 2011 IEEE/ACM International Conference on Green Computing and Communications. IEEE Computer Society, 2011.

[9] Zhao, Huanyu, and Xiaolin Li. "VectorTrust: trust vector aggregation scheme for trust management in peer-to-peer networks." The Journal of Supercomputing 64.3 (2013): 805-829.

[10] G. Theodorakopoulos and J. S. Baras, "Trust evaluation in ad-hoc networks," in Proceedings of the 3rd ACM workshop on Wireless security, 2004, pp. 1–10.

[11] Beth,T., Borcherding, M., Klein, B.: „Valuation of trust in open network".Proc.ESORICS, 1994, pp.3–15

[12] Josang,A.:„A logic for uncertain probabilities" ,Int.J.Uncertainty, Fuzziness, Knowledge-Based Syst., 2001, 9,(3),pp 179–311 13

[13] Mui, L.: „Computational models of trust and reputation: agents,evolutionary games, and social networks". PhDthesis, Massachusetts, 2003

[14] Sun,Y.L.,Yu,W.,Han,Z.,Ray,L.K.J.:„Information theoretic framework of trust modeling and evaluation for ad hoc networks", IEEE J. Sel.Areas Commun., 2006, 24, (2), pp.305–319

[15] Sun,Y.L.,Yu,W.,Han,Z.,Ray,L.K.J.:„Trust modeling and evaluation in Adhoc networks ".Proc. Global Telecommunications, 2005,pp.1–10

[16] Xia, Hui, et al. "Trust management model for mobile ad hoc network based on analytic hierarchy process and fuzzy theory." Wireless Sensor Systems, IET1.4 (2011): 248-266

[17] Satty, T.L.: „The analytic hierarchy process" (McGraw-Hill, New York, 1980)

[18] Xia, Hui, et al. "Trust management model for mobile ad hoc network based on analytic hierarchy process and fuzzy theory." Wireless Sensor Systems, IET1.4 (2011): 248-266

[19] Xia, Hui, Zhiping Jia, Xin Li, Lei Ju, and Edwin H-M. Sha. "Trust prediction and trust-based source routing in mobile ad hoc networks." *Ad Hoc Networks* 11, no. 7 (2013): 2096-2114

[20] Wang, Jian, Yanheng Liu, and Yu Jiao. "Building a trusted route in a mobile ad hoc network considering communication reliability and path length." Journal of Network and Computer Applications 34.4 (2011): 1138-1149.

[21] Ziegler, C.N. and Lausen, G. "Analyzing Correlation Between Trust and User Similarity in Online Communities". Proc. of

the 2 nd International Conference on Trust Management, 2004.

[22] Breese, J. S., Heckerman, D. and Kadie, C. "Empirical analysis of predictive algorithms for collaborative filtering". Proc. of the 14 th Conference on Uncertainty in Artificial Intelligence, 1998.

[23] Herlocker, J. L., Konstan, J. A., Borchers, A., and Riedl, J. "An Algorithmic Framework for Performing Collaborative Filtering". Proc. of the 22nd ACM SIGIR Conference on Research and Development in Information Retrieval, 1999.

[24] Pearson K. "Mathematical contribution to the theory of evolution: VII, on the correlation of characters not quantitatively measurable". Phil. Trans. R. Soc. Lond. A, 195, 1-47, 1900.