July 2011

An Approach for Establishing Trust among Nodes in Ad Hoc Network

Radhika i Sain

Computer Science Department, Ambedkar Institute of Technology, New Delhi, India,
myself_radhika@yahoo.co.in

Manju Khari

Computer Science Department, Ambedkar Institute of Technology, New Delhi, India,
manjukhari@yahoo.co.in

Follow this and additional works at: <https://www.interscience.in/ijssan>

Part of the [Digital Communications and Networking Commons](#), and the [Electrical and Computer Engineering Commons](#)

Recommended Citation

Sain, Radhika i and Khari, Manju (2011) "An Approach for Establishing Trust among Nodes in Ad Hoc Network," *International Journal of Smart Sensor and Adhoc Network*: Vol. 1 : Iss. 1 , Article 8.

DOI: 10.47893/IJSSAN.2011.1007

Available at: <https://www.interscience.in/ijssan/vol1/iss1/8>

This Article is brought to you for free and open access by the Interscience Journals at Interscience Research Network. It has been accepted for inclusion in International Journal of Smart Sensor and Adhoc Network by an authorized editor of Interscience Research Network. For more information, please contact sritampatnaik@gmail.com.

An Approach for Establishing Trust among Nodes in Ad Hoc Network

Radhika Saini¹, Manju Khari²

Computer Science Department, Ambedkar Institute of Technology, New Delhi, India

Email Id: myself_radhika@yahoo.co.in¹, manjukhari@yahoo.co.in²

Abstract— A node in ad hoc network is accountable for routing the packets to neighboring nodes. This evolves trust factor among nodes which assists in forwarding the packets to other nodes if it is trusted and thereby furnishes a secure & reliable communication. This trust can be defined by several approaches which are based on behavior, monitoring, policies etc. In this paper, an approach is proposed to establish trust among nodes which can be evaluated by monitoring the nodes for their behavior. The values are defined for trust which is dynamic in nature and depends on the behavior of nodes.

Keywords- Ad Hoc Network; Nodes; Trust; Malicious Behavior; Attack

I. INTRODUCTION

Ad Hoc Network furnishes wireless connectivity among nodes (like laptop, mobile) to communicate with each other. An example of such ad hoc network is Bluetooth [1]. This communication takes place in open wireless medium and shared radio broadcast channel which makes it vulnerable to attacks [2].

Each node is responsible for the operations like transmitting and receiving the packets, forwarding the packets to neighboring nodes. This decision of forwarding packets evolves the concept of trust among nodes. A packet is sent to the neighboring node if the transmitting node (or the source node) trusts the neighboring node. This packet forwarding procedure is explained through the figure 1 which is given below.

Figure 1 Packet Forwarding

In the above figure 1, N1 is the source node, N2 and N4 are the intermediate nodes and N6 is the destination node. All the links between nodes are wireless. Packets from node N1 is sent to node N6 through node N2 and N4.

Trust among nodes has the following properties [3] -

Subjective – A trustor node may define different level of trust against the trustee node. That is, if a node N1 trust N2

for all processes then it is compulsory that N2 also trusts N1 for all purposes.

Non-Transitive Nature – Trust on node is not transitive in nature. For example in above figure 1, if node N1 trusts N2 and N2 trusts N4 then it is not compulsory that N1 trusts N4.

Asymmetric – A node with higher capability (in terms of computational power and resources) may not trust the node with lower capability. But vice-versa is possible.

Context Dependent – Trust depends on the context. It means that a node may trust other node for one purpose but at the same time does not rely for other purpose.

Dynamic – Trust among nodes can change any time as the node is highly movable in nature. This trust is based on the information about node's behavior.

Such above mentioned properties of trust plays important role in defining trust. More the trust on nodes will be, more will be the reliability and security on the network. This paper is organized as follows: Section II covers the related work on the trust of nodes. Section III describes the design of proposed approach. Proposed approach for trust establishment is given in Section IV. Conclusion and future work is given in Section V.

II. RELATED WORK

Trust between nodes in ad hoc networks can be defined in the following ways [3] –

Reputation based Framework – In this framework, trust among nodes is established on the basis of their reputation. That is, it uses direct and indirect information to evaluate a node.

Trust Establishment Framework – In this, trust is established by taking the opinion from intermediated nodes and also from the direct observation.

Certificate-based Framework – Certificates are issued to the legitimate nodes through a Trusted Third Party (TTP) like Certifying Authority (CA). Based on issued certificates, trust is managed.

Behavior-based Framework – Trust is based on the behavior of nodes. A node can exhibit a normal behavior or malicious behavior. Through this process, nodes are trusted.

Evidence-based Trust Management – It requires some evidence to prove its legitimacy to other nodes through a challenge-response process. This include public keys, addresses etc.

Monitoring-based Trust Management - This defines a level of trust among nodes based on direct and indirect information. Monitoring can be done through Intrusion Detection System (IDS) [4] etc.

Policy-based Trust Management - This concept evolves some security schemes like logical rules etc which is mandatory for a node to pass in order to establish trust among other nodes.

Several researchers have proposed the methods to calculate the trust among nodes which are as follows:

An approach developed for calculating trust between nodes called RTA (Reputation based Trust Management using TGC (Trust Computing Group) in Mobile Ad-Hoc Networks). In this, software composition and configuration is used to calculate the behavior. Reputation is evaluated by an engine and is maintained in a database. [5].

A framework proposed called Adaptive Trust Management in which reputation-based and policy-based approaches integrated into a framework. This framework is capable of furnishing the subjective and objective security. Trust is evaluated based on the past history of nodes and deducing that trust to a value is performed [6].

Another framework proposed called the NTM (Node based Trust Management) which is based on an assumption that every node is accountable for their own trust. This concept changed the trust property of non-transition to transition mode. Moreover, trust value is binary and not a continuous-valued variable. Trust is calculated by Trust Evaluators (TEs) by getting the values of trust [7].

A model proposed in which each node calculates its own trust vector for its neighbour with the help of monitoring the nodes. After this, trust dynamics are calculated for nodes. This model is based on Vector Model of Trust and detects the malicious node based on trust [8].

This Paper is based on monitoring the nodes and behavior based trust management which is used in establishing the trust among nodes.

III. DESIGN OF PROPOSED APPROACH

The proposed approach has three main components – (1) Monitoring of nodes, (2) Table maintaining and updating and (3) Defining trust for neighboring node which is done through (1) and (2) components.

Defining the trust is based on the behavior of nodes. Trust among nodes is developed through monitoring the behavior of nodes. Monitoring of nodes can be done through numerous methods like Random Walker Detector (RWD) [9], Watchdog node [10], Intrusion Detection Systems (IDS) [4] and other several models [11] [12]. When nodes are monitored, each node maintains a table of trust of its neighboring nodes which contains the trust value. This value of trust is dynamic in nature and changes with the behavior of nodes.

IV. PROPOSED WORK

First of all, the value of trust (t) is defined for normal and malicious behavior of nodes.

For Normal Behavior of a node N , $t_N=1$ (1)

For Malicious Behavior of a node N , $t_N=0$ (2)

Under the process of node's monitoring, these above equation may change depending upon the behavior of node. If any legitimate node in normal behavior exhibits malicious behavior then this behavior will be representing by the following equation.

$$t_N \rightarrow 0 \text{ (3)}$$

And if any malicious node starts behaving in a normal behavior, then it is represented by the following equation

$$t_N \rightarrow 1 \text{ (4)}$$

Now to confirm this change in behavior of node, those nodes are monitored for their subsequent behavior to reach a final decision. And their final behavior is represented by the same equations as (1) and (2). The symbol $\rightarrow$ means the value of trust is approaching towards a new value. Equation (3) and (4) are the temporary values based on the behavior of nodes and will be confirmed after monitoring.

Nodes' behavior represented by equation (1) and (2) represents the initial and final behavior of a node. On

finding any node reaching the malicious behavior (i.e. Equation (2)) will be isolated from the network to prevent other legitimate nodes. It is assumed that initially all the node's trust value is 1. That is, all nodes are behaving normally and can be trusted for network operations. Moreover, the value of trust, t is either 1 or 0.

Now this above concept is explained through an example. Below given Figure 2 consists of nodes.

Figure 2 An example of nodes in Ad Hoc Network

Trust among nodes in above figure 2 is determined through above equations. Consider a node, N3 which maintains the table of trust of its neighbouring nodes. The following table1 is maintained at node N3.

Table Maintaining Procedure -

TABLE 1 Table maintained at Node N3

Neighbouring Node	Corresponding Trust Value, t
N1	$t_{N1}=1$
N2	$t_{N2}=1$
N4	$t_{N4}=1$
N5	$t_{N5}=1$

Initial Values at N3 { $t_{N1}, t_{N2}, t_{N3}, t_{N4}=1$ }

In above table 1, all the neighboring nodes of N3 corresponds to value 1 which means all exhibiting normal behavior. Similarly, all the nodes maintain the table of trust for its neighboring nodes.

While monitoring the nodes, if it is found that a node, suppose N4 starts behaving in malicious manner then node N3 updates this formation in its table which is given in table 2.

Table Updating Procedure -

TABLE 2 Table update at Node 3

Neighbouring Node	Corresponding Trust Value, t
N1	$t_{N1}=1$
N2	$t_{N2}=1$
N4	$t_{N4}>0$
N5	$t_{N5}=1$

Updated Values at N3 { $t_{N1}, t_{N2}, t_{N3}=1$ and $t_{N4}>0$ }

If this node N4 continues to behave in the same manner, then trust value is changed to 0 and is updated at the table maintained at N3. This update can be seen in the table 3 which is given below.

Final Values Updating Procedure -

TABLE 3 Table update at Node N3

Neighbouring Node	Corresponding Trust Value, t
N1	$t_{N1}=1$
N2	$t_{N2}=1$
N4	$t_{N4}=0$
N5	$t_{N5}=1$

Final Updated Values at N3 { $t_{N1}, t_{N2}, t_{N3}=1$ and $t_{N4}=0$ }

Thereby, the node N4 is isolated from the network and will not take part in any network operation performed.

This monitoring and final values update can be in other way also. If the node N4 after table updating procedure

exhibits normal behavior again, then this update will be represented by $t_N=1$.

V. CONCLUSION AND FUTURE WORK

In this paper, the trust, t is defined among nodes and is either 1 or 0. $t_N=1$ represents the normal behavior and $t_N=0$ represents the malicious behavior. Any node at value 0 will be isolated from the network. This approach helps in choosing the optimal and secure path for packet forwarding procedure. Therefore, achieves a secure communication.

The working of the proposed approach can be implemented to measure its effectiveness and accuracy. Moreover, it can be measured that to which level this proposed approach helps in determining the trust among nodes in ad hoc networks. Switching of trust values between 1 and 0 can be defined to a different sub values. At $t_N=1$, this trust can be further defined as access level approach.

REFERENCES

- [1] C.Siva Ram Murthy and B S Manoj, —*Mobile Ad Hoc Networks- Architecture and Protocols*, Pearson Education, ISBN 81-317-0688-5 , 2004
- [2] B. Wu et al, —*A Survey of Attacks and Preventions in Mobile Ad Hoc Networks*, *Wireless/ Mobile Network Security*, Springer, Vol 17, 2006.
- [3] Cho, J. Swami, A. and Chen, I. “A Survey on Trust management for Mobile Ad Hoc Networks” *IEEE Communication Surveys & Tutorials*, 2010
- [4] Sahu, S and Shandilya, S K - *A Comprehensive Survey On Intrusion Detection In Manet*, *International Journal of Information Technology And Knowledge Management*, Volume 2, No. 2, pp. 305-310 July- December 2010
- [5] Kpodjedo, S. and Pourzandi, M. “Reputation based Trust Management using TGC in Mobile Ad-Hoc Networks (RTA) *IEEE 2008*
- [6] Yunfang, F. “Adaptive Trust Management in MANET” *International Conference on Computational Intelligence and Security” IEEE 2007*
- [7] Ferdous,R. Muthukumarasamy,V. And Sattar,A. “A Node-based Trust Management Scheme for Mobile Ad-Hoc Networks” *Fourth International Conference on Network and System Security*, *IEEE 2010*
- [8] Gong,W. You,Z. Chen,D. Zhao,X. Gu,M. and Lam,K. “Trust Based Malicious Nodes Detection in MANET” *IEEE 2009*
- [9] Panos,C Xenakis,C and Stavarakis,I - *A Novel Intrusion Detection System for MANETs* *International Conference on Security and Cryptography (SECRYPT) 2009*
- [10] Patcha,A and Mishra,A - *Collaborative Security Architecture for Black Hole Attack Prevention in Mobile Ad Hoc Networks*, *IEEE. 2003*
- [11] Mamatha,G. and Dr. Sharma,S. – *A Highly Secured Approach against Attacks in MANETS*, *International Journal of Computer Theory and Engineering* Vol. 2 No. 5 1793-8201, October 2010
- [12] Bhargava ,B Oliveira,I,R Zhang ,Y and Idika , N - *Addressing Collaborative Attacks and Defense in Ad Hoc Wireless Networks*, *IEEE International Conference on Distributed Computing Systems Workshops*, 2009