International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 9 (2015) pp. 23415-23423

http://www.ripublication.com

Trust Management Scheme for MANET

J. Godwin Ponsam and Dr. R.Srinivasan

Research Scholar, SRM University
godwin.j@ktr.srmuniv.ac.in
Professor Emeritus Directorate of Research SRM University
rsv@yahoo.com

Abstract

Trust management is an approach to provide trustworthiness among any node to node communication. Establishing trust is more difficult in Mobile ad-hoc networks (MANETs) than existing traditional infrastructure based network. In MANET there is no centralized control. Hence no third party can be used. In this paper we have proposed trust management scheme for detecting attacks in MANET. This trust management scheme is based on grey theory. We have evaluated the performance using NS-2 simulator. We have tested for both static and in mobility condition. This trust management system calculates the trust value to detect the abnormal behaviors based on various parameters.

Keywords: grey theory, fuzzy set, attacks

I. Introduction

MANETs are multihop wireless networks with changing network topology. MANETs are small network and can be formed in emergency situations like hostile places. Hence node can be easily compromised. MANET has lot of challenges like limited bandwidth, resource constraint as it is running on battery power and dynamically changing network topology [1]. So establishing trust in manet is a challenging task. In MANET to increase cooperation among nodes, neighbor node should build trust over a particular period of time. In MANET there are huge no. of attacks and there are various solutions have been proposed to prevent some attacks [1]. To prevent attack single layer solutions will not be sufficient and needs multiple layer information to detect a malicious node [2].One major threat in MANET is due to compromised node. Using a compromised node, attacker may execute lots of attacks like sending false routing information. By establishing trust we can detect and isolate an attacker node. In MANET a node has to act as routers as well as source and destination node. MANETs are temporary in nature, because node may join or leave the network

anytime. As nodes are running on battery power, some selfish node may not involve in routing thus leaving network into partition. This type of attack is a passive attack. In black hole attack, the attacker node informs that it has shortest route to destination to divert the traffic to itself. After that malicious node may drop the packet or perform Man in the middle attack. In Gray hole attack an attacker initially agrees to behave correctly but after a while malicious node starts dropping the packet which may lead to a DOS attack. In this paper we have introduced a trust management scheme which considers multiple parameters to calculate the trust value to identify a malicious node. We have used grey theory with whitenization function to detect malicious node. Generally only packet loss rate is used to identify a malicious node. In this scheme multiple parameters are used to detect the attacks.

II. Related Work

Trust management between nodes is done through a central authority or by nodes or in combined. Both these techniques come under related work. Khaled Hamouid and Kamel Adi [15] proposes self certified based trust establishment scheme in adhoc networks. Zhou [8] proposes the idea of utilizing the threshold cryptography to distribute trust in MANET. Davis [7] proposes use of certificates based on hierarchical trust model to manage trust. In reputation based trust model the outcome of the past transactions are stored as trust vectors for other nodes. Trust management framework [10] proposed by N. Li and S. K. Das includes reputation system with watchdog. Watchdog will monitor how many packets are being forwarded and how many acks are received for the sent packet. But in distributed reputation scheme, based on Dampster theory, uses agent feedbacks to indentify the uncertainty. But unfortunately this will not identify the black hole and grey hole attacks. J. Guo, A. Marshall, and B. Zhou [9] proposes a trust management scheme with fuzzy set and this trust management scheme is for static and with limited parameters. Our trust model uses grey theory with whitenization function with multiple parameters with many nodes for both static and mobile nodes.

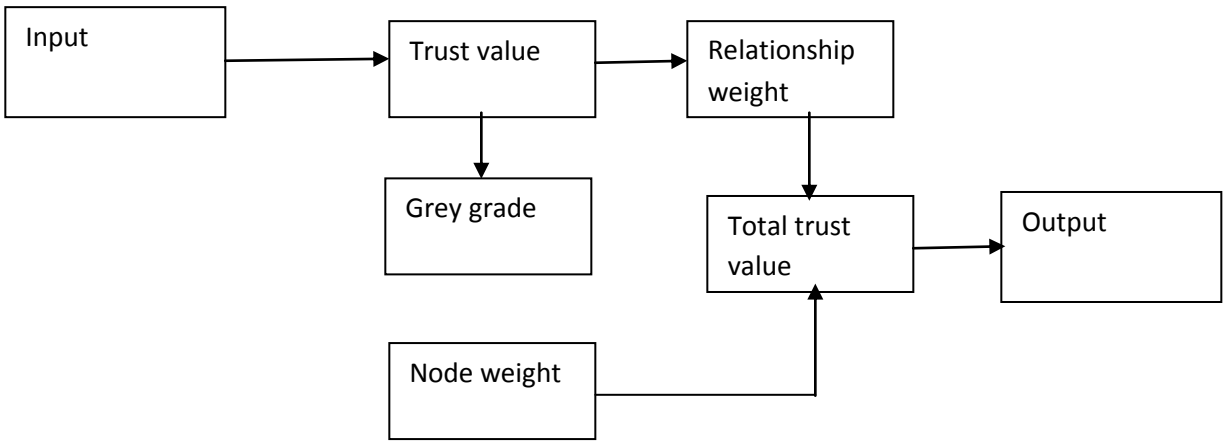

Fig 1. Trust Management Scheme

Trust relationships

In MANET, trust management of the network depends on the node to get trust value. Recent trust management framework views neighborhood as three levels. They are direct trust, indirect trust and recommendation relationships.

Direct trust

Direct trust is evaluated based on the face that previous interactions are successful. For example trust value for node B is calculated based on the successful communication between node A and node B.

Indirect trust

Indirect trust is established through another party node, which is based on the interactions between observed node and one of the observed neighbor node. For example node C, node D, and node G are indirect trust with node A

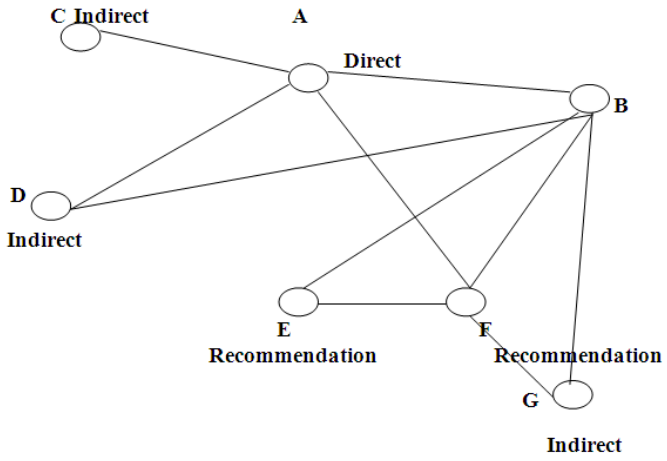

Fig.2 Trust Relationships of nodes

Recommendation trust

This trust is established using an intermediate node called as common node. For example node B and node C will have common node D. If B wants to know the trust record of D through C, C will calculate the trust value of D based on the observations of interaction between C and D.

Trust Formation

Grey Theory

For multiple parameters, like data rate, PLR, signal strength, we can use Grey theory to calculate the trust value. Let X be a grey relational set X=x1,x2,x3. While xi(1,2….n) is an evaluation index. For example this x1 can be PLR, x2 can be signal strength, x3 can be data rate, x4 delay and x5 can be throughput During a time period t=(1,2,…T) from a node point of view for example node A observes the neighboring

node b's behavior and calculates the trust value δ_{ab}=(1,2….n). The framework calculates the node b's sample sequence as yb= { δ ba} and the sample matrix for all the neighboring nodes at period t.

III. Trust Formation

Our trust management system combines the grey theory and fuzzy sets for calculating the trust value. This trust management framework designed to be robust against many attacks.

Grey Theory

Based on grey theory we can calculate the trust value. From Grey theory, let there be a grey relational set x={x1,x2,x3….xn}. x= {packet loss rate, signal strength, packet delivery rate, delay, throughput}.

After some time period from the view of a node **x** which observes the neighbor node **a** and calculates its trust value. This framework will get the nodes sample sequence xi. After some time period t, the best trust value sequence A=(a1,…ai…an) while ai= best chosen value. Also the worst value sequence B=(b1,…bi…bn).bi is the worst chosen value. Based on Grey theory we can obtain the Grey relation coefficient of the best trust value and worst trust value.

$$\{\theta,\varphi\}=\frac{\mathbf{minj|\partial ji-\{a,b\}i|+\rho maxj|\partial ji-\{g,b\}i|}}{\mathbf{\partial|ji-\{a,b\}i+\rho maxj|\partial ji-\{a,b\}i|}}$$

At time period t, node b's best and worst value will be

$$\{\theta,\varphi\}j=\Sigma_i=vi\{\theta,\Phi\}j,I \qquad (2)$$

From the above equations when normal settings ρ=1/2 the grey value ranges from .33 to 1. To normalize the value between [0,1]. For that we can convert the values using mappings y=1.5x-.5. Then using least square methods the TMF can obtain the node a's trust value in view of node b.

Trust value Computation

The overall trust value is computed based on fuzzy set. We followed the approach to identify the trust of a node based on its historical behavior and we get the trust value based on classes of grey clusters.

The following are the classes of grey clusters.

A1 Not trusted
A2 Min trust
A3 Trusted

Whitenization function

$$f1(x) = \begin{cases} 1, x <= .30 \\ -4x/3 + 4/3, x > .25, \end{cases} \quad x1 = .25 \tag{3}$$

$$f2(x) = \begin{cases} 2x, x <= .5 \\ -2x + 2, x > .5, \end{cases} \quad x2 = .5 \tag{4}$$

$$f3(x) = \begin{cases} 4x/3, x <= .75 \\ 1, x > .75, \end{cases} \quad x3 = .75 \tag{5}$$

When node **x** gets trust value of node **y** from different nodes. The Whitenization weight of trust value $T_{xK.}$ T_{xK} is the trust value of x evaluated by node k.

$$Tjk = \frac{1}{1+(\varphi j)^2} \ / (\theta)^2 \tag{6}$$

If $\max_s\{f_s(T_{BK})\}$ is between certain value grey cluster class is A2,
If $\max_s\{f_s(T_{BK})\}$ is under the value then A1 then not quite trusted
If $\max_s\{f_s(T_{BK})\}$ is above the value then the class is A3 quite trusted.
The total trust value for node K is

$$\text{Total } T = \frac{1}{2}(\max\{fj(Tdirect)\}) + \frac{1}{2} \frac{2NR}{2NR+N1} \sum \frac{wk}{\sum wk} (\max\{fj(Tk)\})Tk + \tag{7}$$

$$\frac{1}{2} \frac{N1}{2NR+N1} \sum \frac{wk}{\sum wk} (\max\{fj(Tk)\})Tk$$

IV. Discussion and Analysis

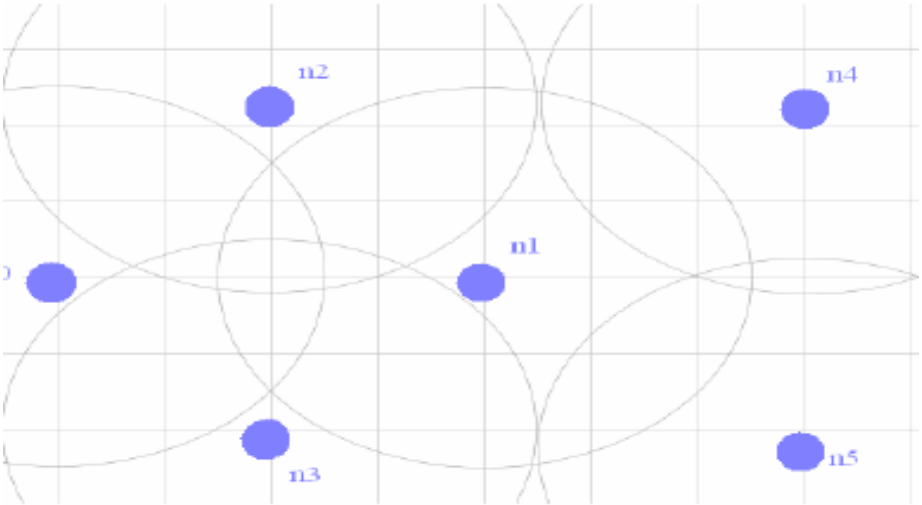

Fig. 3 Topology

Topology of nodes

We have analyzed the performance using ns2 simulator. In this simulation AODV routing protocol is used for routing packets. For this simulation we have used around 6 mobile nodes. Node 1 gets the trust value from other nodes 2,3,4,5 and 6. The size of each data packets is 120 bytes. The parameters used for observations are delay, throughput, PLR(packet loss rate). Data rate used is 1 Mbps. In each scenario it took 5 seconds to reach from node 1 to node 2 to get the trust value. In fig.3 each second the simulator calculates the grey trust value. In fig 4. The PLR is shown due to PDR

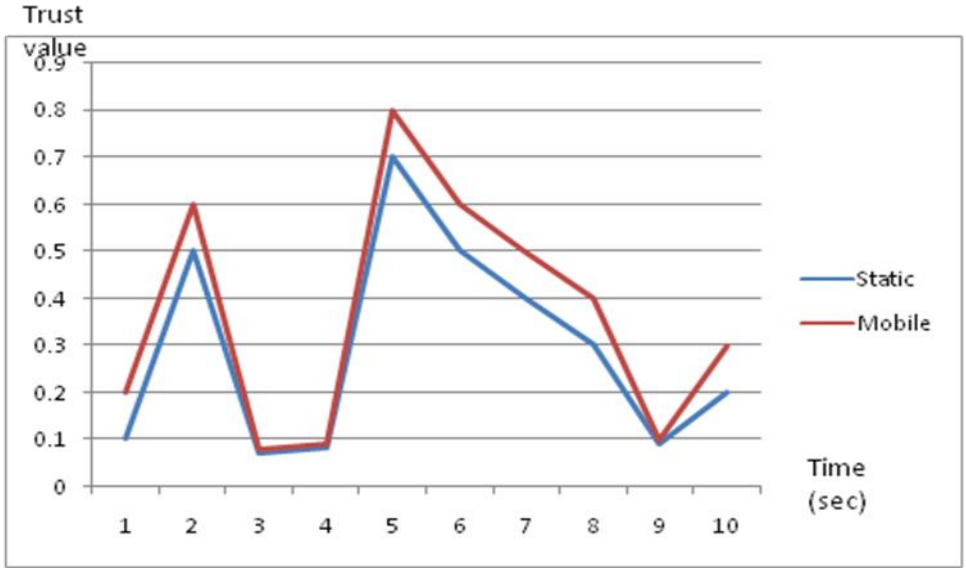

Fig. 4. Trust Values

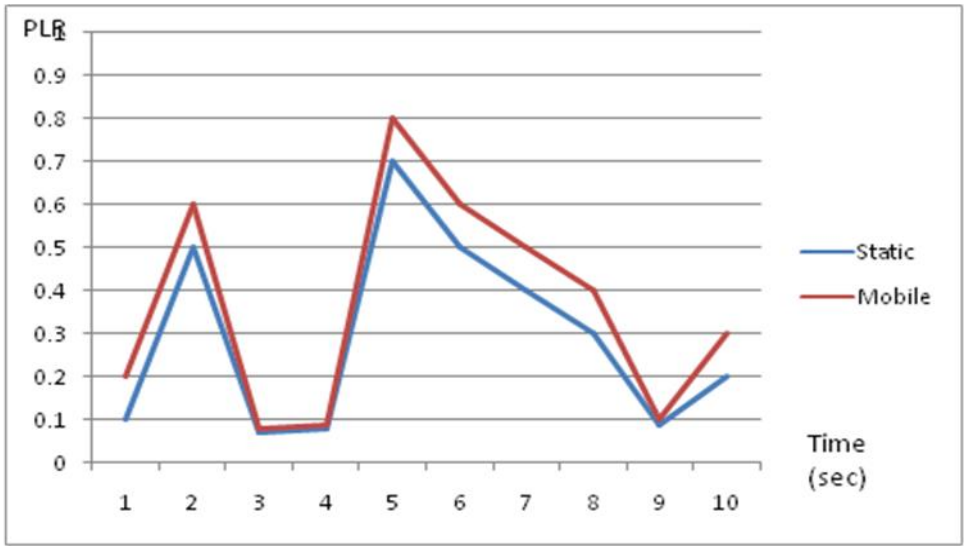

Fig.5 Trust values and PLR

Total Trust values

The trust value for node 1 is calculated. We have included direct trust, indirect trust and recommendation trust obtained from other set of nodes for node as T1, T2 and T3.

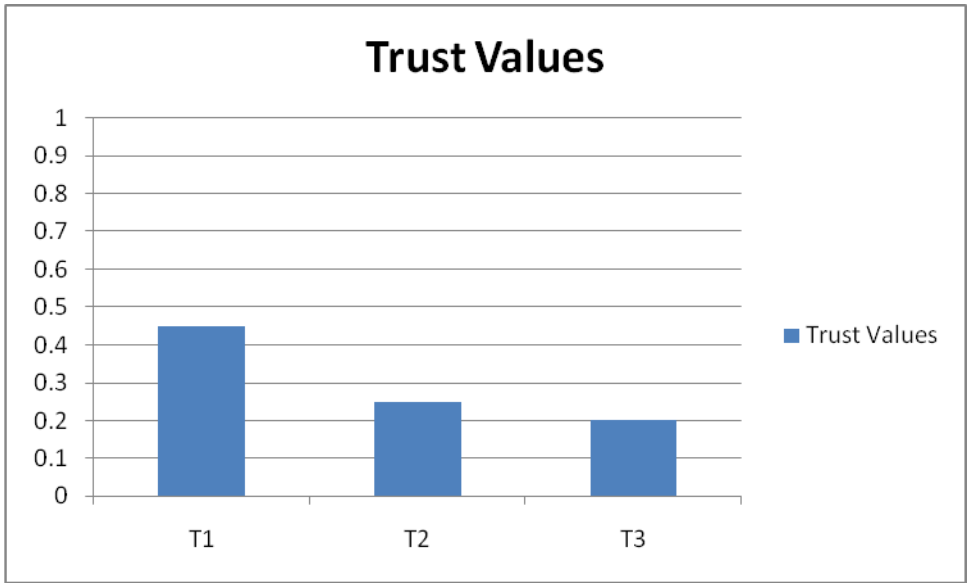

Fig. 6. Trust Values

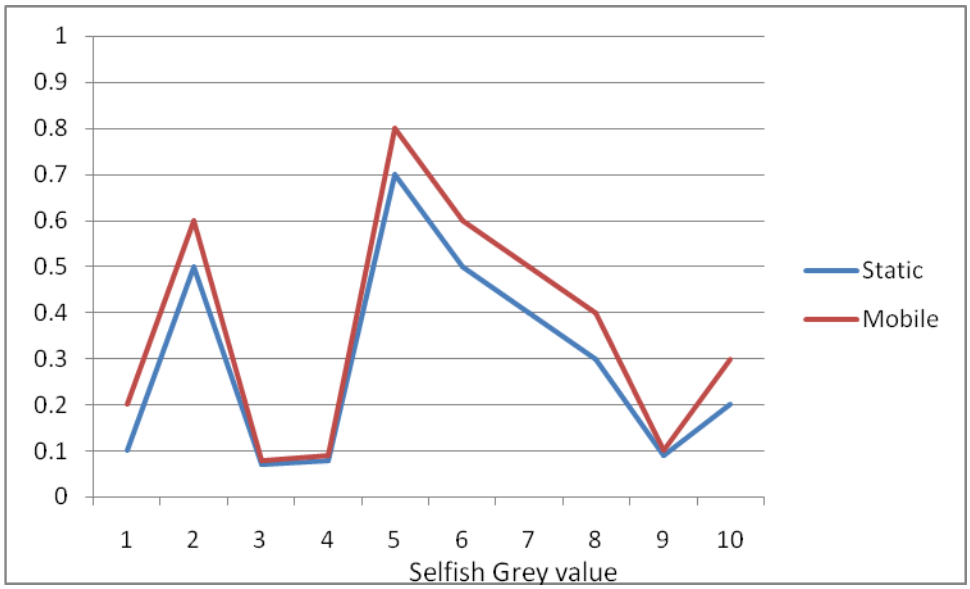

Fig.7. Selfish Grey value

Selfish behavior

Weight vectors {A} are used to find the grey value and framework calculates the trust

value. These trust values helps to find the abnormal and normal behavior. We have considered the packet loss rate, signal strength, delay, and throughput and data rate parameters.

Weight vectors
A1= {.4, .4,.4,.4,.4} all parameters set to same weight
A2= {.4, .1,.1,.1,.1} PLR
A3= {.2,.6,.2.,.2,.2} signal strength
A4={.3,.3,.3,.3,.6}delay
A5={.1,.1,.1,.6,.1}PDR

Using this framework we can identify the abnormal behavior also we can identify the parameters responsible for it. Mostly the node can find the difference in trust value between normal node and selfish node when the parameter has equal values. By using

V. Conclusion

In this paper we have introduced a trust management scheme which identifies selfish node which comes under passive attack. In existing scheme which uses only PLR to find the selfish node but using new trust management scheme we have used many parameters to find the selfish node. We have used Grey theory with whitenization function to calculate the trust value. Simulation results show the difference between normal and abnormal behavior of nodes. Our future work is to find the combined attacks in MANET.

VI. References:

1. J. Godwin Ponsam, R.Srinivasan, " A Survey on MANET Security Challenges, Attacks and its Countermeasures, in IJETTCS, 2014

2. J.Godwin Ponsam, R.Srinivasan,"Multilayer Intrusion Detection in MANET", IJCA,vol.no. 2015

3. Cai, F., Fugui, T., Yongquan, C., Ming, L., Bing, P.: Grey Theory Based Nodes Risk Assessment in P2P Networks. In: IEEE International Symposium on Parallel and Distributed Processing with Applications, pp. 479–483 (2009)

4. Sun, Y.L., Han, Z., Liu, K.J.R.: Defense of Trust Management Vulnerabilities in Distributed networks. IEEE Communications Magazine 46(2), 112–119 (2008)

5. Li, H., Singhal, M.: Trust Management in Distributed Systems. IEEE Computer Society 40, 45–53 (2007)

6. Qin, Z., Jia, Z., Chen, X.: Fuzzy Dynamic Programming based Trusted Routing Decision in Mobile Ad Hoc Networks, Embedded Computing. In: Fifth IEEE International Symposium on Embedded Computing, SEC 2008, pp. 180–185 (2008)

7. C. Davis. A localized trust management scheme for ad hoc networks. Proceedings of 3rd International Conference on Networking (ICN'04). Mar. 2004.

8. L. Zhou and Z.J. Haas. Securing ad hoc networks. IEEE Network Magazine, vol. 13, no. 6, pp. 24-30, November 1999

9. J. Guo, A. Marshall, and B. Zhou," A Trust Management Framework for Detecting Malicious and Selfish Behaviour in Ad-Hoc Wireless Networks Using Fuzzy Sets and Grey Theory" Springer 2011, p.p277-289

10. N. Li and S. K. Das, "A trust-based framework for data forwarding in opportunistic networks", Ad Hoc Networks, Elsevier, 2012

11. Y. Wang, J. Vassileva, Trust and reputation model in peer-to-peer networks, In Proc. Third Int'l Conf. Peer-to-Peer Comput. (P2P'03), Linkoping, Sweden, Sep. 2003, pp. 150-157.

12. C. Davis. A localized trust management scheme for ad hoc networks. Proceedings of 3rd International Conference on Networking (ICN'04). Mar. 2004

13. L.Eschenauer, V.Gligor and J. Baras. On Trust Establishment in Mobile Ad-Hoc Networks,Proceedings of 10th International Workshop of Security Protocols, Springer Lecture Notes in Computer Science (LNCS), Apr. 2002

14. J. Li, R. Li, and J. Kato, Future Trust Management Framework for Mobile Ad Hoc Networks: Security in Mobile Ad Hoc Networks, IEEE Communications Magazine, vol. 46, no. 4, Apr. 2008, pp. 108-114.

15. D. Johnson and D. Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks, Mobile Computing, T. Imielinski and H. Korth, Ed., Kluwer, 1996

16. Khaled Hamouid and Kamel Adi ,"Self-Certified Based Trust Establishment Scheme in Ad-Hoc Networks " International Conference on NTMS 2012