ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

An Efficient Distributed Trust Model for Detecting Selfish Nodes

Anju Markose[1], Vidhya P.M[2]

Final Year M.Tech Student, Dept. of CSE., Sree Narayana Gurukulam College of Engineering, Kerala, India[1]

Assistant Professor, Dept. of CSE., Sree Narayana Gurukulam College of Engineering, Kerala, India[2]

ABSTRACT: A mobile Ad Hoc network is a collection ofmobile nodes. They do not have any existing infrastructure and they do not have any centralized administrator. So the MANET is self-creating, self-organizing and self-administrative wireless network. In MANET each node acts as router. In practice some of the nodes may act as the selfish nodes. These nodes use the network and its services but they do not cooperate with other nodes. Such selfish nodes do not consume any energy such as CPU power, battery and bandwidth for retransmitting the data of other nodes. They will preserve the resources for their own use. The use of watchdogs is a well-known mechanism to detect selfish nodes. However, the detection process performed by watchdogs can fail, generating false positives and false negatives that can induce to wrong operations. A way to reduce the detection time and to improve the accuracy of watchdogs Trust Based Model can be used.

The trust model has become important for malicious nodes detection in MANETs. It can assist in any applications such as secure routing, secure data aggregation, and trusted key exchange. Due to the wireless features of MANETs, it needs a distributed trust model without any central node, where neighbour nodes can monitor each other. In addition, an efficient trust model is required to handle trust related information in a secure and reliable way. Here, a distributed and efficient trust model named EDTM was proposed. During the EDTM, the calculation of direct trust, recommendation trust and indirect trust are discussed. Furthermore, the trust propagation and update are studied. Trust models have been recently suggested as an effective security mechanism for Mobile Adhoc Networks (MANETs). First, according to the number of packets received by nodes, direct trust and recommendation trust are selectively calculated. Then, communication trust, energy trust and data trust are considered during the calculation of direct trust. Furthermore, trust reliability and familiarity are defined to improve the accuracy of recommendation trust.
.

KEYWORDS: EDTM; MANETs;

I. INTRODUCTION

Ad Hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any centralized administration, in which individual nodes cooperate by forwarding packets to each other to allow nodes to communicate beyond direct wireless transmission range. Routing is a process of exchanging information from one station to other stations of the network. Routing protocols of mobile ad-hoc network tend to need different approaches from existing Internet protocols because of dynamic topology, mobile host, distributed environment, less bandwidth, less battery power. Mobile ad hoc network is a self-configuring infra-structure less network of mobile devices connected by wireless links. Ad hoc in Latin means “for this purpose”. Each device in a MANET is free to move independently in any direction and will change its links to other devices frequently. Each must forward traffic unrelated to its own use and act as a router. The primary challenge in building a MANET is to equip a device to continuously maintain the information required to properly route the traffic. They may operate themselves.

The trust model has become important for malicious nodes detection in MANETs. It can assist in any applications such as secure routing, secure data aggregation, and trusted key exchange. Due to the wireless features of MANETs, it needs a distributed trust model without any central node, where neighbour nodes can monitor each other. In addition, an efficient trust model is required to handle trust related information in a secure and reliable way. Here, a distributed and efficient trust model named EDTM was proposed. During the EDTM, the calculation of direct trust, recommendation trust and indirect trust are discussed. Furthermore, the trust propagation and update are studied. Trust models have been recently suggested as an effective security mechanism for Mobile Adhoc Networks (MANETs). First, according to the

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

number of packets received by nodes, direct trust and recommendation trust are selectively calculated. Then, communication trust, energy trust and data trust are considered during the calculation of direct trust. Furthermore, trust reliability and familiarity are defined to improve the accuracy of recommendation trust.

II. RELATED WORK

A MANET is a rapidly growing technology based on self-organized and rapidly deployed network. MANET have different real life applications because of its distinctive features. In [5, 6] the authors reviewed that many researchers are trying to remove main limitations of MANET like limited bandwidth, battery power, computational power etc. In the literature reviewed, trust has been used in such heterogeneous networks like WSNs, MANETS for assessing the availability, reliability, and security countermeasures through identifying compromised nodes based on past interaction experiences, [7] [8] [9] [10] proposed reputation-based framework for data integrity in WSNs considering that system takes information collected by each node using a Watchdog mechanism to detect invalid data and uncooperative nodes. Yao et al. [11] proposed an energy-efficient communication protocol for wireless micro sensor networks based on parameterized trust. Bharghavan, V., Demers, A., Shenker, S., And Zhang, L. Macaw [12] proposed a media access protocol for wireless LAN. Here also he proposed some trusted and secured protocol for wireless network. Cho al [13], present a complete survey on trust management. In trusted computing concept, devices always perform as per expectation i.e. imposed both by hardware and encryption software. Trusted Computing Group (TCG) defined Mobile Trusted Module (MTM) [14,15] to provide a specification of encryption or decryption, signature generation and sensitive data storage to deliver functions such as secure boot, data integrity, device authentication and remote verification as security assurance cannot be randomly established between two nodes that are previously unknown to one another in an heterogeneous and doubtful situation. Pirzada and McDonald [16] projected a trust model to evaluate trust of each node in MANETs. In this approach the trust value is evaluated with a continuous range from -1 to +1. Negative value for trust can occur as a result of more failures than success for various events such as data forwarded, data received, control packets forwarded and etc. But their trust evaluation is basically based upon only direct data communication of each node to other nodes.
Bhalaji and A. Shanmugam [11] proposed a Dynamic Trust Based Method to Mitigate Grayhole Attack in Mobile Ad-hoc Networks. They proposed a new routing protocol based on the trust model. Here each node calculates trust value and association status for all its neighboring nodes through monitoring its behavior in the network. They have incorporated their trust model into the existing Dynamic Source Routing (DSR) protocol. They have proposed it for Gray hole Attack and claimed that they are able to made 17% improvement compared to standard DSR

III. PROPOSED ALGORITHM

If the number of packet drop nodes increases then the data thrashing would also likely to be boost . A malicious node can initiate the following two attacks:
PACKET SINKING: A malicious node slump all or a few of the packets that is believed to beforward. It can also sink the data produced by itself on behalf of some malicious intention for instance.
PACKET AMENDMENT: A malicious node alters the entire or a few of the data packets thatis made- up to forward. It can also modify the data it produce to defend it from being recognized or to lay blame on former nodes.
In previous Black hole detection techniques, black hole node is randomly chosen based on the number of packet dropped. So, sometime legitimate user also treated as the intruders or attacker. It will result into high false positive rate and it violates the security of wireless networks.
TRUST VALUE ALGORITHM: The proposed algorithm is based on the trust values ofindividual nodes. Initially, all the nodes of wireless ad-hoc network have zero trust value. The algorithm comprises the following steps:

- **Initialization:**

  Trust values of all the participating nodes are initializing with zero.
  Initialize the threshold value of the trust value with 100.
  Assumption: 1 trust value = 10 packets dropped.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

- **Updating of trust values:**

1. If the packets are correctly transmitted from one node to another node:

a. If the correctly transmitted number of packets is between 1 to 10, then trust values of the respective nodes will be incremented by one time.
b. Updated trust value = old trust value + 1;
c. If the correctly transmitted number of packets are greater than 10, then the updated
d. trust value will be:
e. Updated trust value = old trust value + (correctly transmitted packets / 10);
2. If the packets are dropped/delayed :
a. The number of dropped or delayed packets is between 1 to 10, then trust value of that particular node is decremented by one.
b. Updated trust value = old trust value – 1;
c. The number of dropped or delayed packets are greater than 10, then trust value of that particular node will be,
d. Updated trust value = old trust value **–** (Packet dropped or delayed / 10);
3. If the trust value of particular node is negative, then print "Invalid node".

III. Isolating the Packet drop node from the network:

If (Updated trust value <<< Threshold trust value)
Then the particular node is treated as malicious node (Black hole node)
If (Updated trust value > Threshold trust value) Then the particular node is treated as legitimate node.
Stop comparing the trust values of nodes with threshold value.

In our approach, we detect the black hole node based on the trust values (Proposed trust value algorithm). We used Traffic pattern Analysis Techniques and associate trust values with each wireless nodes. Initially, all nodes has 'zero' trust value. If the particular node is not involving in packet drops, then each time the trust value of corresponding node will increase by 1.

IV. PSEUDO CODE

.
TSRM (S, T, N_i, TM, α, 🡭)

// **S is the source node**
// **T is the target node**
// **N_i is the neighboring nodes**
// **TM is the trust evaluation matrix**
// **→is sending**

// **α is the threshold value**

{ Step 1: S🡭RREQ to N_i.

Step 2: $N_i$checks TM withα. **Step 3:** If value of TM of N_i> **α**
N_i🡭RREQ to its neighborsContinue until T is reached.

Step 4: If some $N_i$responds route to T,Then S checks the TM of some N_i and choose the best route.
Step 5: S🡭data packets to T using theroute.
T 🡭 confirmation message.
Step 6: If within the time slot, T's confirmationarrives S will continue sending data packets using the route.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Else If T's confirmation cannot receive within the preferred time slot,
S will update its trust evaluation matrix data by reducing the trust value.
Else If the source node makes sure the response node of underlying route is malicious, it will put the node into the intrusion black list, set that value to -1.

Step 7: The source node selects the second best routeand then goes to **step 4** and repeat. }

V. SIMULATION RESULTS

In this effort, we have tried to assess the special effects of the Packet Drop attacks in the Wireless Ad-hoc Networks. To attain this we have replicated the wireless ad-hoc network set-up which contains packet drop node using NS2 Network Simulator program. To create the packet drop node in a wireless ad-hoc network we have employed fresh protocol that jump down data packets after be a magnet for them to itself.

TABLE 1: SIMULATION PARAMETERS

Parameter	Specification
Simulation tools Used	NS2 Network Simulator (NS 2.35), Exata
Simulation Time	10 sec, 20 sec
Number of Nodes	20,40,60,80,100
Transmission Range	250 m
Maximum Speed	0-22 m/sec
Application Traffic	CBR(Constant Bit Rate) [20]
Packet Size	512 Bytes
Node Mobility Model	8 Packets/sec
Protocol	AODV
Number of runs	12
Threshold trust value	100

To obtain correct results from the simulations, we applied UDP protocol. The source node remains on carriage out UDP packets, although the nasty node goes down them, while the node terminates the link if it makes use of TCP protocol. As a result, we may possibly examine the connection flow between sending node and receiving node throughout the simulation.

We simulated 10 different network scenarios having different number of nodes. We observe the simulation results to get the values of various network parameters like throughput, Packet drop ratio (PDR), Packet delivery ratio (PDLR), Average trust value and false positive rate (FPR). Various graphs are plotted to observe the relationship between these parameters.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

TABLE 2: EXPERIMENT DATA WITH 10 DIFFERENT SCENARIOS

Scenario	Nodes	Throughput (mbps)	FPR	PDR	Avg. trust value	PDLR
1	10	2.793	0.013	0.013	91.42	0.987
2	20	2.923	0.042	0.019	85.63	0.967
3	30	2.897	0.061	0.027	81.03	0.943
4	40	2.453	0.097	0.074	76.45	0.912
5	50	2.307	0.153	0.156	72.09	0.893
6	60	2.109	0.196	0.162	71.73	0.796
7	70	2.908	0.173	0.159	72.95	0.776
8	80	2.003	0.237	0.204	69.78	0.709
9	90	1.459	0.214	0.193	70.05	0.698
10	100	1.763	0.349	0.297	63.50	0.635

PDLR: Packet delivery ratio PDR: Packet drop ratio FPR: False positive rate

Figure 1 shows the variation of throughput against packet delivery ratio. Here, the throughput increases with increasing packet delivery ratio. Figure 8 shows that the FPR also increases as the PDR increases.

Figure 2 shows the effect of PDR on the trust values. It clearly implies that as the PDR increases the trust value deceased in an almost linear way. The node which acquires its trust value equal to or more than the threshold value is considered a legitimate node.

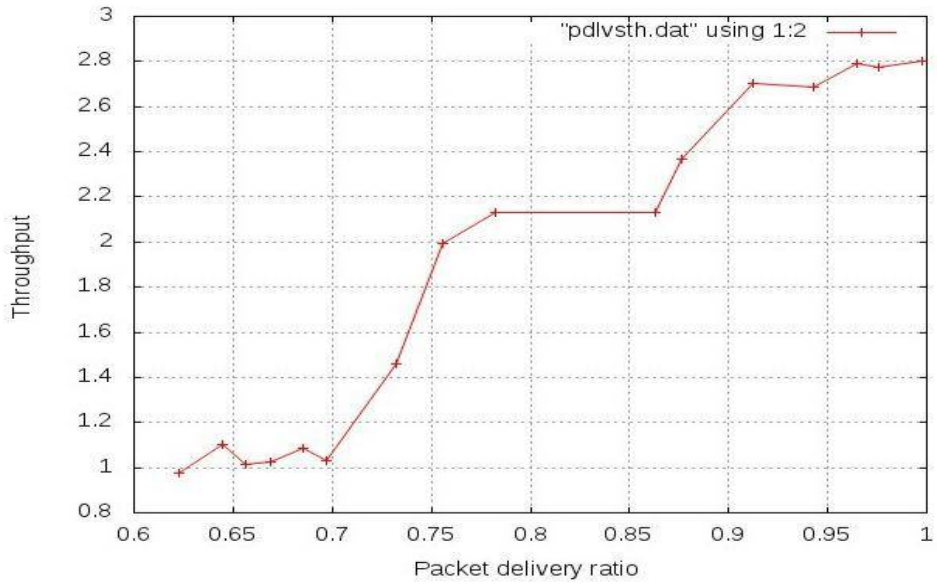

Figure 1: Throughput Vs Packet delivery ratio

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

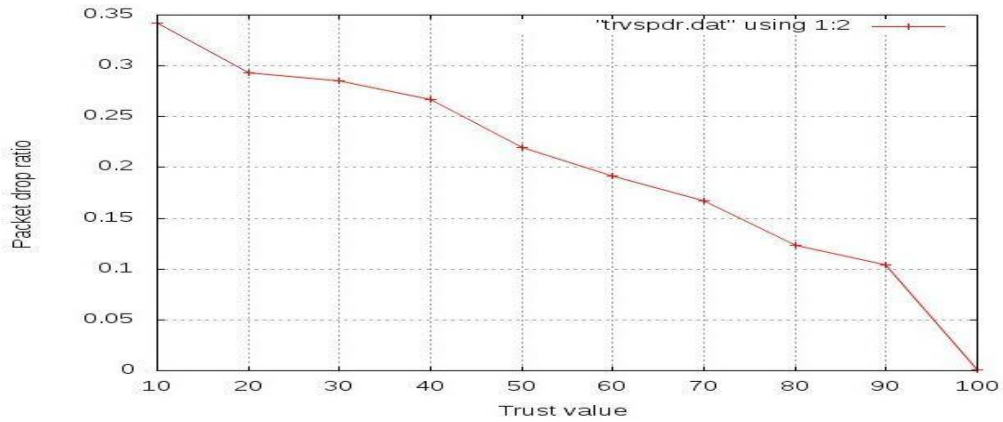

Figure 2: Packet Drop Ratio Vs Trust value

VI. CONCLUSION AND FUTURE WORK

While designing a new trust system, it is necessary to consider the constraints and the type of information that can be used as input by the network. A general observation is that so far, the existing research work and proposals lack completeness. There are important issues yet to be addressed. Some of them include:

• **Impact of network dynamics on trust:** Though, we have given a brief outline about impact of network dynamics on the various trust dynamics, the detailed analysis of the impact has to be addressed. For example, mobility can impact the trust propagations and various other security paradigms. But the clear quantifiable relationship is yet to be determined. Similarly, the relationship between other network dynamics (including link dynamics, network density) and trust and its dynamics are yet to be analysed.

• **Computations of trust in cooperative and non-co-operative games:** In a self-organized distributed network, nodes can give positive or negative recommendations about others either genuinely or maliciously with some self-interest. These aspects are analogous to situations in complex systems with game theoretic interactions. The games can be non-cooperative where every node plays game independently or cooperative where a set of nodes form sub groups and play game together against the rest of nodes. Non cooperative games are tractable using Nash equilibrium. Trust computation with cooperative game is not well analysed yet. The earlier attempts are preliminary in nature and these attempts exploits the collaborations in positive way to obtain the trust scores.

• **Impact of heterogeneous nodes on trust:** Wireless networks could be highly heterogeneous. The heterogeneity could be in terms of the roles of the nodes, their inherent capability and security. Heterogeneity implies that not all nodes or their contents can be treated equally when it comes to trust evaluations. Thus, the same functional descriptions will not be applied to evaluate the trust levels of all nodes and their information. Investigation is needed on incorporating network dynamics and heterogeneity in the trust evaluation functions.

• **Security paradigms to enhance trust in the network:** The data delivery capabilities and security properties of the network directly impact the level of trust a recipient places on the information received. As an example, it is possible that a piece of information cannot be fully trusted unless its source and the path over which it is received are authenticated. If authentication services are not available one must decide whether to have the untrusted information or none at all. Further research is required to characterize these metrics through modelling efforts and to determine the degree to which security properties influence the network trust.

• **Social and context dependent trust:** Social relationship and context based trust by establishing social communities among entities has received considerable attention in recent days. However, this is still unexplored area with respect to MANET. The complex dependence between the communications network, the social network, and the application network is not yet explored in MANET. The social communities can also help in validating the trust measurements. Validation of measured trust is another major area of future research.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

REFERENCES

[1] E. M. Royer and C-K Toh , "A review of Current routing protocols for Ad Hoc Mobile Wireless",2002.
[2] I. Chlamtac, M. Conti, and J. J. N. Liu, "Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks", pp. 6-13, 20
[3] Fenye Bao, Ing-Ray Chen, Moon Jeong Chang, and Jin-Hee Cho; "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection", IEEE Transactions on Network And Service Management, Vol. 9, No. 2, June 2012.
[4] J. Lopez, R. Roman, I. Agudo, C.G. Fernandez, "Trust Management Systems for Wireless Sensor Networks: Best Practices", Computer Communication. 2010;33:1086–1093.
[5] J. H. Cho, A. Swami, and I. R. Chen, "A survey on trust management for mobile ad hoc networks," IEEE Communication Surveys Tutorials, vol. 13, no. 4, pp. 562–583, 2011.
[6] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, "Secure Routing and Intrusion Detection in Ad Hoc Networks", In Proceedings of the 3rd International Conference on Pervasive Computing and Communications (Kauai Island, Hawaii, March 2005), IEEE, pp. 191.199.
[7] W.R. Heinzelman, A Chandrakasan, H Balakrishnan, "Energy-efficient communication protocol for wireless micro sensor networks". Proc. 33rd Hawaii International Conference on System Sciences, 1–10 (2000).
[8] V. Bharghavan, A. Demers, S. Shenker, and L. Zhang, "Macaw: a media access protocol for wireless LAN's". In Proceedings of the conference on Communications architectures, protocols and applications (1994), ACM Press, pp. 212.225.
[9] M. Y. Hsieh, Y.M. Huang, H.C. Chao, "Adaptive Security Design with Malicious Node Detection in Cluster-Based Sensor Networks", Computer Communication 2007;30: 2385–2400.
[10] A.A. Pirzada, and C. McDonald, "Establishing trust in pure ad-hoc networks", in Proceedings of the 27th conference on Australasian computer science. Dunedin, New Zealand: Australian Computer Society, 2004.
[11] N. Bhalaji, A.Shanmugam "Dynamic Trust Based Method to Mitigate Grayhole Attack in Mobile Ad-hoc Networks", International Conference on Communication Technology and System Design, Procedia Engineering 30, pp. 881 – 888, 2012.
[12] Z. Yan, P. Zhang, and T. Virtanen. "Trust Evaluation Based Security Solution in Ad Hoc Networks", in Proceedings of the Seventh Nordic Workshop on Secure IT Systems Norway, 2003
[13] M. Virendra, *et al.* "Quantifying Trust in Mobile Ad-Hoc Networks" ,in International Conference on Integration of Knowledge Intensive Multi-Agent Systems, 2005 (KIMAS '05) Waltham, Massachusetts, USA: IEEE,2005.
[14] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey on trust and reputation management systems in wireless communications" Proceedings of the IEEE, vol. 98, no. 10, pp. 1755–1772, 2010.
[15] Mawloud Omara, *et al.* "Reliable and fully distributed trust model for mobilead hoc networks" computers & security 28, Pp. 199-214, 2009.
[16] Marcela Mejia, *et al.* "A game theoretic trust model for on-line distributed evolution of cooperation in MANETs" Journal of Network and Computer Applications 34, pp. 39–51, 2011.
[17] Feng Zhang, *et al.* "Node trust evaluation in mobile ad hoc networks based on multi-dimensional fuzzy and Markov SCGM(1,1) model" Computer Communications 35, pp. 589–596, 2012.
[18] T.W.A. Grandison, "Trust Management for Internet Applications", in Department of Computing, University of London: London, British. pp. 252, 2003.

BIOGRAPHY

Anju Markose is a Final year MTech student, Sree Narayana Gurukulam College of Engineering.