www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume2 Issue 8 August, 2013 Page No. 2641-2644

Trust Aware AODV

V.Vallinayagi[1] Dr G.M, Nasira[2]
Dept of CS, SSC COLLEGE, T.N 627011,INDIA
Dept of CA, TIRUPUR, T.N 627012, INDIA

ABSTRACT:
The advantage of Mobile Ad-hoc Networks (MANETs) is to form a wireless network in the absence of fixed infrastructure. . In defining and managing trust in a military MANET, we must consider the interactions between the composite cognitive, social, information and communication networks, and take into account the severe resource constraints. We provide a survey of trust management schemes developed for MANETs and discuss generally accepted classifications, potential attacks, performance metrics, and trust metrics in MANETs. Finally, we discuss future research areas on trust management in MANETs based on the concept of social. AODV node is able to discover multiple loop-free paths as candidates in one route discovery. These are evaluated by two values hop count and trust values. In this paper we discuss about trust value and improves the packet ratio

Keyword: Manet,aodv trustvalue,path,time

INTRODUCTION:

In traditional wireless networks, a base station or access point facilitate communications betweennodes with the Network and Communications with destinations outside he network. In contrast, MANETs forms a network in the absence of fixed infrastructures. The requirement of these networks is only nodes that can interact with radio hard wares so as to route the traffic using the routing protocol. Thus the reduced essential requirement s of such networks, along with their adoptability into tiny resource-limited devices made them more popular and is much preferred for several applications in the area of communications.

Routing protocols determines the nature of data forwardness as well as its adaptability to topology changes that results by mobility. Initial MANET routing protocol like AODV [1]was not designed to withstand malicious nodes within the network or outside attackers near by with malicious intent. Subsequent protocols and protocol extensions have been proposed to address the issue of security Many of these protocols seek to apply cryptographic methods to the existing protocols in order to secure the information in the routing packets. This attack is very effective in MANETs, as the devices often have limited battery power in addition to the limited computational power.

There are two primary motivations associated with trust management in MANETs. Firstly, trust evaluation helps identify malicious entities. One entity can remember others behaviors through evaluation history. This memory provides a method for good entities to avoid working with 'ex-Convict' or suspected ones. Secondly, trust management offers a prediction of one's future behaviors and improves network performance. The results of evaluation can be directly applies as an incentive for a good or honest behavior while a penalty for a selfish or malicious behavior in the network. The feedback reminds network participants to act with caution.

In table II the time, storage and communication complexity are given for different and hoc routing protocols. Time complexity is defined as the number of steps needed to perform a protocal operations, Storage Complexity measures the order of the table size used by the protocols and Communication Complexity gives the number of messages needed to perform an operation when an update occurs.

Parameters	**On - Demand**	**Table - Driven**
Availability of routing information	Available when needed	Always available regardless of need
Periodic route updates	Not required	Required.
Copying with mobility	Use localized route discovery as an ABR and SSR.	Inform other nodes to achieve a consistent routing table.
Signaling traffic generator	Grows with increasing mobility of	Greater than that of on – demand routing

	active routes.	

Protocal	Time Complexity	Storage Complexity	Communication Complexity
DSDV	O(d)	O(X)	O(N)
CGSR	O(d)	O(N/M)	O(N)
WRP	O(h)	O(X*A)	O(N)
AODV	O(2d)	O(E)	O(2N)
DSR	O(2d)	O(E)	O(2N)
TORA	O(2d)	O(D_d*A)	O(2A)

Where,
N=Number of nodes in the network
d=Network diameter
E=Communication pairs
M=Average number of nodes in a cluster
X=Number of nodes affected by topological Change
H=Height of routing tree
A=Average number of adjacent nodes
D_d=Number of maximum desired Destination

2. NODE'S TRUST VALUE CALCULATION

Measuring the trust value of the node is always a challenging problem [14&15].A nodes trustworthiness is often related to the quality of services it provides to others. If the quality of the service can be objectively measured, then entities trustworthiness for that service is called objective trust.

Most of the previous research used the approach of subjective trust. Then they classified the trust relation as direct and indirect relation. The direct trust relation of a node is related to its neighbors while the indirect trust relation is concerned with the non-neighbors.

RF_N (M)(Request-for-Forwarding);The total no of packets that node N has transmitted to node M for Forwarding.

HF_N (M) (Has-Forwarded):The total no of packets that have been forwarded by node M and is noticed by node N.

The two no are updated by the following rules. When node N sends a packet to node M for forwarding, the counter RF_N (M) is increased by one. Then node N listens to the wireless channel and check whether node M forwards the packet as expected. If node N detects that node M has forwarded the packet before a preset time –out expires , the counter HF_N (M) is increased by one.

Trust value calculation basic scheme drawbacks :(1) Increased nodes power consumption because it assumes that each node operates in promiscuous mode to monitor its neighbors continually. (2)Flooding the network by broadcasting the updated evaluations consumes the network limited band with. (3) The broadcasted evaluation records come from misbehaving nodes which leads to wrong results. (4) Taking into consideration the credibility of node i which broadcasts its evaluation record about node X when calculating OER(X) leads to computational overhead. (5) It does not take into account a node's "selective forwarding" behavior, where it only forwards small packets while selectively discarding larger ones.

Route's Evaluation

Each sending node S builds its own trust evaluation table Teval(S) using the propagated trust values in the network. T Eval(S) contains the trust value of all other in the network. Using these trust information, the sending node routing agent ROA(S) is responsible for computing the most trustworthy route to a particular destination. If the most trustworthy route trusts value is found lower than a threshold value (denoted by R threshold). The route is rejected and a new Route Discovery process is initiated. The trust value in route R by source node S is represented as Ts(R) and given by the following equation: Ts(R) =min(Trust-value(Ni)) $\forall$ Ni ε R (4)

3. COMPUTATION OF NODE TRUST:

The trust of a node j in another node k (node trust for short) is a measure to ensure that packets sent by node j have actually been forwarded by node k. Two trust factors [CFR (t) and DFR (t)] are assigned weights in order to determine the overall trust value of a node. The direct trust in node k by node j is represented as T_{jk} and is given by the following formula

$$T_{jk}(t) = w_1 \times CFR_{jk}(t) + w_2 \times DFR_{jk}(t) \quad (2)$$

Where CFR_{jk} (t) and DFR_{jk} (t) represent control packet forwarding ratio and data packet forwarding ratio observed by node j for forwarding node k at time t, respectively. The weights w1 and w2 (w1,w2 $\geq$ 0 and w1+ w2=1) are assigned to CFR and DFR, respectively. Node k forwards the packet correctly. If so, the trust value T_{jk} increases. Otherwise, T_{jk} decreases. In our trust model, trust values are limited in a continuous range from 0 to 1 (i.e. $0 \leq T_{jk} \leq 1$). The trust value of 0 signifies complete distrust whereas the value of 1 implies absolute trust. If there is no interaction between two nodes, the initial trust value is set to 0.75 which is minimum trust. A threshold n termed as the blacklist trust threshold is used to detect malicious node In other words if the trust value is smaller than n it is regarded is malicious nodes.

4. Proposed system:

In this paper consider trust model
Which lives on time line? Many protocols consider certain nodes as normal and certain are malicious node because existing node's
Behavior changed. so the trust will be recalculated. Each node is given specific time in that time the node behavior is tested
Soothe trust is calculated based on the control packets and data packets transmission initially to find the routes of the nodes. Trust value calculates the transmission of data packets. So every windows calculate the number of data packets and control packets>0

5. Experiment results:

We have conducted a comprehensive test using ns2 2.34 and all experiments are done on a pc personal computer with pIV
The graph is shown for finding the performance activity. When 1000*1000 grid lines, we disperse 100 nodes

Time window	Max Trust obtained
To	0.75
T1	0.79
T2	0.81
T3	0.83
T4	0.85
T5	0.88

Table.1

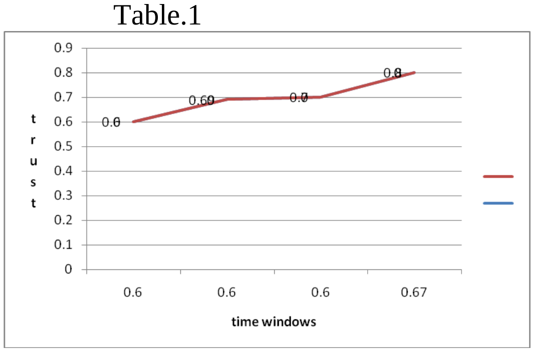

Fig 2

In fig2 based on time window, the level of the trust is incresed gradually by isolating the no of malicious nodes from the network.

No of nodes	Malicious nodes
10	4
30	3
50	10
70	8

Table2

Based on the number of nodes and the transmission from one node to another node,the trust values can be deviated in every transmission.

Conclusion

Thus this paper considering the evolution of trust on demand adaptive trust windows model to increase the delectability of no of malicious nodes

References:

[1] Son, B., Her, Y., Kim, J., "A Design and Implementation of Forest-Fires Surveillance System based on Wireless Sensor Networks for South Korea Mountains", IJCSNS International Journal of Computer Science and Network Security, vol.6 No.9B, 124–130, September 2006.
[2] Mainwaring et al, "Wireless Sensor Networks for Habitat Monitoring", International Workshop on Wireless Sensor Networks and Applications (ACM), Sep. 2002,
[3] Chintalapudi, K.; Fu, T.; Paek, J.; Kothari, N.; Rangwala, S.; Caffrey, J.; Govindan, R.; Johnson, E.; Masri, S., "Monitoring civil structures with a wireless sensor network," *Internet Computing,IEEE* , vol.10, no.2, pp. 26-34, March-April 2006
[4] Ian F. Akyildiz, Tommaso Melodia, Kaushik R. Chowdhury, "A survey on wireless multimedia sensor networks", *The International Journal of Computer and Telecommunications Networking*, Vol. 51 , Iss. 4, March 2007, pp. 921-960.
[5] V. C. Giruka, M. Singhal, J. Royalty, S. Varanasi, "Security in wireless sensor networks", *Wirel. Commun. Mob. Comput.* 2008; 8:1–24.
[6] T.Kavitha, D.Sridharan, "Security Vulnerabilities In Wireless Sensor Networks: A Survey"*Journal of Information Assurance and Security*, Vol. 5 (2010) 031-044.
[7] Jaydip Sen, "A Survey on Wireless Sensor Network Security", *International Journal of Communication Networks and Information Security (IJCNIS)* Vol. 1, No. 2, August 2009.
[8] Chris Karlof, David Wagner, "Secure routing in WSNs: attacks and ountermeasures", Ad hoc networks Journal, vol. 1, Issue 2-3, Sept. 2003, pp.293-315.
[9] G. Padmavathi, D. Shanmugapriya, "A Survey of Attacks: Security Mechanisms and Challenges in Wireless Sensor Networks", (IJCSIS) *International Journal of Computer Science and*

Information Security, Vol. 4, No. 1 & 2, 2009.
[10] Asad Amir Pirzada, Chris McDonald, and Amitava Datta "Performance Comparison of Trust-Based Reactive Routing Protocols", *IEEE Transactions on Mobile Computing*, Vol. 5, No. 6, June 2006.
[11] Y. Sun, Z. Han, K. J. RAY Liu, "Defense of Trust Management Vulnerabilities in Distributed Networks", *IEEE Communications Magazine*, February 2008, pp: 112–119.
[12] Sencun Zhu, Sanjeev Setia, Sushil Jajodia. "LEAP: Efficient Security Mechanisms