ISSN No. 0976-5697

Volume 4, No. 8, May-June 2013

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Manet Source Routing Model Based On Trust Security

Umasankar Mohandoss
Dr A Kumaravel, Prof AR Arunachalam
Dept. of Computer Science Engineering, Bharath University, Chennai, India
umasankarm@gmail.com

Abstract: Mobile adhoc network consists of only nodes and they don't have any fixed or centralized controlling infrastructures since there is no centralized controlling infrastructure in the network each node in this MANET has to depend on other nodes to forward the packets and it also paves way to security issues which brings challenges to researchers. Since absence of previous information of nodes participating in the network to ensure the information and resources access provided only to trusted nodes there should be a formulation need to be done to find the trust of each nodes participating in the network. Many Secure solutions has been proposed - In this paper we propose the trust based sourcerouting modeland simulate and compare with the existing dsr model

Keywords: MANET,ADHOC, Trust based source routing,

I. INTRODUCTION

The advantage of the adhoc network is that it can be deployed anywhere without depending on any existing infrastructure.Mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless network. In MANET there is no centralized controlling architecture but it can be deployed in places where we cannot establish a wired network like a disastrous environment Military application etc. As the topology of the MANET is changing time to time in a dynamic fashion it is prone to variety of security threats. These attacks on MANETs challenge the mobile infrastructure in which nodes can join and leave easily with dynamics requests without a static path of routing. Schematics of various attacks as described by Al-Shakib Khan [1] on individual layer are as under: Application Layer: Malicious code, Repudiation Transport Layer: Session hijacking, flooding Network Layer: Sybil, Flooding, Black Hole, Grey Hole. Worm Hole, Link Spoofing, Link Withholding, Location disclosure etc.

Data Link/MAC: Malicious Behaviour, Selfish Behaviour, Active, Passive, Internal External Physical: Interference, Traffic Jamming, Eavesdropping In spite of lot of deployments of MANET are sensitive to the message transmitted in Application layer, it has a lack of security in Network Layer and Mac Layer . Most of security attacks such as black hole and grey hole are addressing the routing procedure and it blocks the packets forwarded to its neighbouring nodes. Many security schemes from different aspects of MANETs have been proposed, such as secure routing protocols [2],[3], [4], [5], [6] and solutions for secure key management [7], [8], [9], [10], [11]. In our model we present the trust model which is very flexible and it is applicable to MANET.

In our trust model trust information of nodes is calculated and it based on previous transaction history and knowledge of individual nodes and its recommendations acquired for the neighbouring nodes that plays a great role to improvise the process of trust evaluation. This trust evaluation process eliminates the broken link or outage in any resource based on the information of transaction done by the other nodes which in turn results in predicting and isolating the nodes with malicious behaviours which helps us to stop forwarding the packets to those identified malicious nodes also it yields another function which allow us to determine the node with higher trust value and based on this the nodes also learn the identified trusted nodes to build a trust repository also it is not forwarding the recommendation to the other nodes thus eliminates the possibility of false recommendations. Possessing the other nodes information regarding the trust implies less energy consumption and less processing power for calculation of trust with minimal memory requirements Also due to mobility nature of nodes in MANET the topology of the network also changes dynamically which make it difficult to maintain the record about all the nodes[12] in the MANET.

The organization of this paper is in such Section II contains details about the Black Hole ,Dynamic Source routing protocol and computation of route trust and Section III contains our model and the results are shown in Section IV and the final Section 5 contains the conclusion.

II. DSR PROTOCOL

The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. The protocol is composed of the two main mechanisms of "Route Discovery" and "Route Maintenance", which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network. All aspects of the protocol operate entirely on demand, allowing the routing packet overhead of DSR to scale automatically to only what is needed to react to changes in the routes currently in use. Theprotocol allows multiple routes to anydestination and allows eachsender to select and control the routes used in routing its packets,for example, for use in load balancing or for increased robustness. Other advantages of the DSR protocol include easily guaranteed loop-free routing, operation in networks containingunidirectional links,use of only "soft state" in routing, and very rapid recovery

whenroutes in the network change. The DSR protocol is designed mainlyfor mobile ad hoc networks of up to about two hundred nodes and isdesigned to work well even with very high rates of mobility.

The DSR protocol is consists of two main mechanisms Route Discovery and Route Maintenance that work together to allow the discovery and maintenance of source routes in the ad hoc network:

Route Discovery is the mechanism by which a node A wishing to send a packet to a destination node E obtains a source route to E. Route Discovery is used only when A attempts to send a packet to E and does not already know a route to E.

Route Maintenance is the mechanism by which node A is able to detect, while using a source route to E, if the network topology has changed such that it can no longer use its route to E because a link along the route no longer works. When Route Maintenance indicates a source route is broken, A can attempt to use any other route it happens to know to E, or it can invoke Route Discovery again to find a new route for subsequent packets to E. Route Maintenance for this route is used only when A is actually sending packets to E.

When a node A wants to send messages to node E, it firstly broadcasts (RREQ) a route request which contains the destination and source nodes' identities. Each nodes in between that receive RREQ will add its identity and rebroadcast it until RREQ reaches a node N who knows a route to E or the node E. Then a reply (RREP) will be generated and sent back along the reverse path until node A receives RREP. When node A sends data packets, it adds the path to the packets' headers and starts forwarding. During route maintenance, A detects the link failures along the path. If it happens, it repairs the broken links. Otherwise, when the source route is completely broken, node A will restart a new discovery.

Route Maintenance [14] is the mechanism by which source node is able to detect, while using a source route to destination node, if the network topology has changed such that it can no longer use its route to destination node because a link along the route no longer works. When Route Maintenance indicates a source route is broken, source node can attempt to use any other route it happens to know to destination node, or can invoke Route Discovery again to find a new route. Both Route Discovery and Route Maintenance each operate entirely on demand.

Black holes refer to places in the network where incoming traffic is silently discarded (or "dropped"), without informing the source that the data did not reach its intended recipient. When examining the topology of the network, the black holes themselves are invisible, and can only be detected by monitoring the lost traffic.

A infected malicious node sends fake routing information, claiming that it has an valid route to the destination and causes other good nodes to route data packets through the malicious node hence the attacker consumes or intercepts the packet without any forwarding also attacker can completely modify the packet and generate fake information, this cause the network traffic diverted or dropped

A. Route Trust computation:

When the source node found a route to the destination node with the help of the nodes which forwards the packets then we can determine the trust value for the route using the trust values of the nodes in that specific route. In our model the Route Trust RT (denoted as TR*(ti)*) should be equal to minimum one of the node values in the route

$$RT\ (ti) = MIN\ (\{Tmn(ti) \mid Xm, Xn \in P \text{ and } Xm \rightarrow Xn\}) \quad (1)$$

Where P is the Route andXm, Xn are the neighbouring nodes on the route and Xm → Xn refers Xn is next hop node of Xm

The trust computation based on minimal value is similar to opinions in information theory: the information cannot be increased via propagation [15]

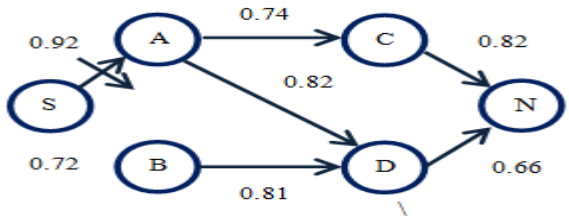

Figure 1 Route Trust Computation

The above graph shows the branches between the source node S to the destination node N via three paths out of that the path S->A->C->N is the highest trusted path

III. TRUST MODEL

In our trust model we sum up all the trust computed values in linear way from the trust calculated from the nodes in the route also the nodes learn neighbouring node trust information by recommendations which is used to derive the Route trust as well.

A. Trust computation:

We can define the trust computation using the trust values from node x to node y similar to Virendra et al. [16].

The fundamental equation

Weighted sum of trust be T*x*(*y*) then knowledge and the recommendations of neighbour's, can be derived as

$$T_x(y) = W1xQ_x(y)+W2xK_x(y)+W3xR_x(y) \quad (2)$$

Where Qx(y) gives the trust node *x* has on node *y* and the ranges will be from [0, 1]

Considering the information on of experience gained by the nodes or we can refer as knowledge gained by the nodes,$K_x(y)$ is the knowledge of node *x* about node *y*which ranges from [0, 1] and $R_x(y$ is the sum of the recommendations trust value gained from the from all other neighbouring nodes of node a which also has the range from [0, 1]. The variables W1, W2 and W3 that ranges from [0, 1], and W1+W2+W3=1, are parameters in our model that allows nodes to choose the most relevant factor. In our model, the value of $Q_x(y)$ is given by

$$Q_x(y)= \Delta E_x(y)+(1-\Delta)T_x(y) \quad (3)$$

$E_x(y)$ is the computed trust value of node *x* to node *y* monitored at node *y*

$T_x(y)$ is the value of the last trusted information from the trust table.

Δ represent factors of different weights ranging form values [0,1]

$$E_x(y) = \frac{P_y^{ogp}}{P_y^{ogp}+P_y^{icp}} \quad (4)$$

Where

P_y^{ogp} is outgoing packets from node *y*

P_y^{icp} is the all the incoming packets to node y

Based on the previous trust computation for the trust level recommendation from the neighbouring nodes now we can able to determine or specify a specific threshold value and whichever the nodes trust value above that specific trust value can be trusted and if multiple nodes got higher threshold values on the route computation then the nodes of higher trust value (threshold) with shortest path can be determined and the routing should be calculated based on that also we need to include the packet loss parameter to determine the amount of packet loss between the nodes.

$$RT_x(y) = \frac{\sum_{(n \epsilon \tau)} NT_n(y)\ CTV}{\sum_{(n \epsilon \tau)} CTV} \qquad (5)$$

Where $CTV = NT_x(y) RC_n(y)$

$RT_x(y)$ is node x evaluation to node y with adjacent nodes recommendation about the node y τis the trusted recommended group

$RC_n(y)$ Relationship computed threshold between the nodes n and y CTV represent the computed trust value

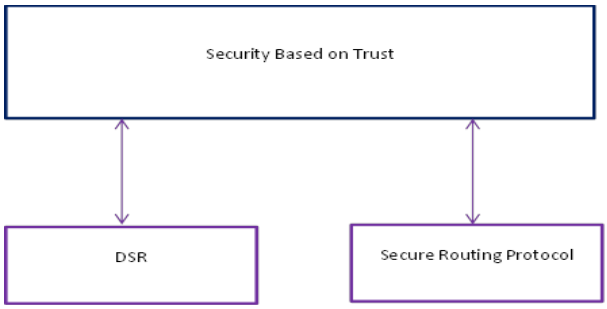

Figure: 2

IV. CONCLUSION

In this paper we proposed the secured trust based source routing model which learns itself from the previous information about the node history and the recommendations also even if the recommendation is high but the current trust value is below the threshold still it is able to avoid those broken link and nodes which provides a flexible and feasible approach to predict the better route which remarkable than the traditional dsrmodel.”This is proposed model only” but this proposed model need to be simulated in ns2 and need to be compared with dsr and aodv protocols

V. REFERENCES

[1]. Tomas Krag and Sebastian Büettrich (2004-01-24). "Wireless Mesh Networking". O'Reilly Wireless DevCenter.Retrieved 2009-01-20.

[2]. M. G. Zapata and N. Asokan, “Securing ad hoc routing protocols,” in Proceedings of ACM Workshop on Wireless Security (WiSe ’02). Atlanta, USA: ACM Press, September 2002, pp. 1–10, http://doi.acm.org/10.1145/570681.570682.

[3]. Y.-C. Hu, A. Perrig, and D. B. Johnson, “Ariadne: A secure on-demand routing protocol for ad hoc networks,” in Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MobiCom ’02), Atlanta, USA, September 2002, http://citeseer.nj.nec.com/article/hu02ariadne.html.

[4]. H. Yang, X. Meng, and S. Lu, “Self-organized network layer security in mobile ad hoc networks,” in Proceedings of ACM Workshop on Wireless Security (WiSe’02), Atlanta, USA, September 2002.

[5]. K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, “A secure routing protocol for adhoc networks,” citeseer.nj.nec.com/551839.html.

[6]. Y.-C. Hu, D. B. Johnson, and A. Perrig, “Sead: Secure efficient distance vector routing in mobile wireless ad hoc networks,” in Proceedings of 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA ’02), June 2002, pp. 3–13, http://citeseer.nj.nec.com/hu02sead.html.

[7]. S. Capkun, L. Buttyan, and J.-P.Hubaux, “Self-organized public-key management for mobile ad hoc networks,” in Proceedings of ACM Workshop on Wireless Security (WiSe ’02), Atlanta, USA, September 2002, http://citeseer.nj.nec.com/capkun02selforganized.html.

[8]. L. Zhou and Z. J. Haas, “Securing ad hoc networks,” Journal of IEEE Networks, vol. 13, no. 6, pp. 24–30,1999.

[9]. J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, “Providing robust and ubiquitous security support for mobile ad-hoc networks,” in Proceedings of IEEE ICNP ’01, 2001.

[10]. J.-P. Hubaux, L. Buttyan, and S. Capkun, “The quest for security in mobile ad hoc networks,” in Proceedings of ACM Symposium on Mobile Ad Hoc Networking and Computingi (MobiHoc ’01), 2001.

[11]. H. Luo, P. Zerfos, J. Kong, S. Lu, and L. Zhang, “Selfsecuring ad hoc wireless networks,” in Proceedings of IEEE ISCC ’02, 2002

[12]. B. Ishibashi and R. Boutaba, “Topology and mobility considerations in mobile ad hoc networks," Ad Hoc Netw. J., vol. 3, no. 6, pp. 762-776, Nov. 2005.

[13]. www.ietf.org/rfc/rfc4728.txt

[14]. K.Selvavinayaki, K.K.Shyam Shankar, Dr.E.Karthikeyan “Security Enhanced DSR Protocol to Prevent Black Hole Attacks in MANETs” International Journal of Computer Applications (0975 – 8887) Volume 7– No.11, October 2010

[15]. Sun, Y., Yu, W. ,Han, Z.,and Liu, K.J.R.:’Information Theoretic Framework of Trust Modeling and Evaluation for AdHoc Networks’, IEEE Journal on Selected Areas in Communications, 2006, 24, (2),pp. 305-317

[16]. M. Virendra, M. Jadliwala, M. Chandrasekaran, and S. Upadhyaya, “Quantifying trust in mobile ad-hoc networks," in Proc. IEEE International Conf. Integration Knowledge Intensive Multi-Agent Syst., Waltham, USA, Apr. 2005