A survey on Trusted Agent-based On-Demand Routing Protocol in MANET

Preeti Bhati
Department of CSE
MRIU, Faridabad
versatilepreeti1986@yahoo.com

Rinki Chauhan,
Department of CSE
MRIU, Faridabad
iknirs@gmail.com,

***Abstract*—Ad-hoc wireless networks are self-organising, infrastructure less networks characterized by dynamic topology, limited channel bandwidth and limited battery power at the nodes. The nodes communicate with each other through radio links in multihop specified routing protocols. The concept of agent is introduced in MANET to reduce the load on node .The routing performance in Mobile Ad-hoc Networks (MANETs) relies on the co-operation of the individual nodes that constitute the network. The existence of misbehaving nodes may paralyze the routing operation in MANET. To overcome this behavior, the trustworthiness of the network nodes should be considered in the route selection process combined with the hop count. The trustworthiness is achieved by measuring the trust value for each node in the network. In this paper we have considered trusted agent based routing mechanism in two reactive protocols and presented the analysis of trusted agent in the extensions of Ad-hoc on Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) routing protocols in MANET.**

***Keywords*—MANET, multipath routing protocol, AODV, DSR, agents, trustworthiness.**

I. INTRODUCTION

Ad-hoc network consists of a set of wireless nodes that are connected by wireless links without any based station or infrastructure support. Mobile Ad-hoc Network [1] is collection of mobile nodes which communicate with each other via multi hop wireless links. Therefore a distinct feature of mobile ad-hoc network is there reduced dependence on infrastructure. MANET routing protocols are classified into three broad categories: table driven (proactive), on-demand (reactive) and hybrid protocol [12]. In MANET, all nodes are act as a router and host at the same time. The MANET network nodes are highly dynamic in nature (behaviour). Due to which its consequences of mobility and disconnection of mobile host poses a number of problems in designing proper routing scheme for effective communication and routing between nodes. It is very difficult for a node to perform routing and communication between nodes efficiently due to heavy responsibilities. Now the concept of agent is introduced to manage the node responsibilities. We have discussed the reason why the concept of are agent are introduced in MANET.

In general, routing protocols for MANET are designed based on the assumption that all participating nodes are fully cooperative. Due to MANET characteristics such as limited battery power, mobility, dynamic topology and limited channel bandwidth, these may be targeted by attackers in a number of ways [3]. Several "secure" routing protocols have been proposed for MANET [4] [5]. Most of them assume centralized units or trusted third-parties which actually destroy the self-organization nature of MANET. These protocols are efficient to fight against external attacks, but are not able to prevent selfishness like misbehaviors problems of node etc. For example, a node may refuse to forward data packets for other nodes to save its battery. So a comprehensive approach is necessary for MANET to prevent from both attacks and misbehavior problems. This is achieved by developing mechanisms for measuring the trustworthiness of the network nodes. The measure of the trustworthiness of such nodes is analyzed by a term called trust level, which is called trusted routing protocols.

II. RELATED WORK

We have analyzed ATDSR [8] [13] protocol (to manage trust information locally with minimal overheads) and TAODV [7] [15] (it focuses on subjective logic to protect routing behaviors in the network layer of MANET). Both these protocols are based on the idea of preventing the MANET from attacks and routing misbehaviors. Also ATDSR and TAODV have achieved higher rate of success over the basic on-demand routing protocols.

The remainder of this paper is organized as follows. We have described the basic reactive protocols i.e. AODV and DSR in section 3. The version of basic DSR and AODV named as ATDSR and TAODV respectively are described in details in section 4. Conclusion is made in section 5.

III. ON-DEMAND ROUTING PROTOCOLS

The reactive protocols have been discussed intensively in the literature and have been found to

have much less routing overhead in comparison to overheads in proactive protocols. Among the reactive protocols, DSR and AODV protocol has been very useful and effective. Therefore, before discussing about extensions such as ATDSR and TAODV we briefly discusses basic on-demand routing protocols.

A. AODV

AODV routing protocol [16] [12] is a reactive. AODV is based on-demand routing scheme which states that it (nodes) discovers a path only when the need arises. AODV requires host node to maintain only active routes. An active route is used to forward at least one packet within the past time out period. It is free from loops, by using the concept of sequence numbers to ensure that chosen route is always fresh enough for routing.

In AODV, each node maintains a routing table which contain one route entry for each destination that the node is communicating with. It has two phases: Route Discovery and Route maintenance. Route Discovery: when the host node needs to send a packet to destination and doesn't contain an active route to the destination node in its routing table. It broadcast a route request (RREQ) packet to its neighbors. During the process of forwarding the RREQ packet, all the intermediate nodes record, in their routing tables, the address of neighbor from which the first copy of the broadcast is received, thereby establishing the reverse path. When the RREQ reaches the destination or an intermediate node with fresh enough route, the destination/intermediate nodes responds by unicasting a route reply (RREP) packet back to the neighbor from which it first received the RREQ The second phase for AODV is the route maintenance, where routes are maintained in the following manner: if a source node moves, it is able to reinitiate the route discovery process to find a new route to the destination node. Also if a node along a route moves, its upstream neighbors notice the move and propagates a ink failure notification or route error message (RERR) to each of its active neighbors so that they can update their routing table.

B. DSR

Under DSR protocol, as mentioned in [2] [6] all control packets contain transmitted for path discovery for the complete list of nodes that form a route to destination node D. Source node S broadcasts a route REQUEST (RREQ)packet containing a unique identification number and the IP address of D. When it receives first copy of the RREQ packet, a node that has no route to D appends its IP address to the RREQ packet and rebroadcasts it after incrementing the TTL field. When a RREQ reaches to the D, a node which has a route to D, a route Reply (RREP) packet that contain the IP address of every node forming the route is returned to S. Several RREP packets can be issued by D. Nevertheless, a node forwards only the first RREP packet it receives and consequently multiple node disjoint paths can be established between S and D. If a link brakeage occurs and results in the incapacity of forwarding, node to reach the destination, a route ERROR (RERR) packet is sent to the source. All nodes that have no alternate path to D update their routing table according to the RERR packet information and forwarded the RERR packet to S.

IV. ATDSR AND TAODV ON –DEMAND ROUTING PROTOCOLS

In this section we are describing briefly extensions of AODV and DSR named as TAODV and ATDSR respectively.

A. Agent-Based Trusted Dynamic Source Routing (ATDSR) Protocol

Agent-based Trusted Dynamic Source Routing (ATSDR) [8] [13] an on-demand routing protocol which uses source routing. ATDSR finds the most trusted as well as minimum hop-count route out of the possible different routes in terms of overheads. It uses a Multi Agent System (MAS) which consists of two types of agents monitoring agent (MOA) and routing agent (ROA).Both of these agents work together to achieve the task assigned by a host node. MOA is responsible for monitoring the host node behavior as well as computing the trust value of this node in the routing process. ROA is assigned to use the trust value which is computed by MOA and find the most trust worthy path for a particular destination node.

1) System Assumptions

There are certain assumptions defined are as:

a) Every participating node in the network must install its Multi Agent System (MAS) which consists of monitoring agent (MOA) and routing agent (ROA).

b) All the trust computations' are maintained locally the nodes MOA.

c) The agents are re4bound to unauthorized analysis and changes of their computation and messages.

2) Node Trust Value Calculation

The node trust value computation is always challenging because of dynamic topology of MANET. Node trust value is related to the quality of services it provides to other nodes in the network. To show the node's selective forwarding behavior, ATDSR compute Trust_Value (N) as:

where,

$$\text{Trust-Value (N)} = \frac{\text{FN(N)*pkt-size(FN(N)}}{\text{FT (N)*pkt-size (FT (N)}}$$

FN (N): total number of packets that have been forwarded by node N.

FT (N): total number of packets that all nodes have transmitted to node N for forwarding.
Pkt-size (FT (N): total size of packet FN (N)
Pkt size (FT (N): total size of packet FT (N)

For each arbitrary node Ni, its MAS, locally maintains a trust evaluation table with the help of T-V (N). The trust value is calculated by the above mentioned formula. Mobile agent has the duty of calculative this T-V (N) and passes this value back to the stationary agent in the host node. Therefore finds the most trusted as well as minimum hop-count route out of the possible different routes in terms of overheads.

B. Trusted AODV (TAODV)

TAODV [7] [15] is a trusted routing protocol for secure transmission of data in MANET.TAODV is a routing protocol based on applying the trust model into security solutions of MANET. The trust and trust relationship among nodes can be represented, calculated and combined for efficient routing. A self–organized key management scheme such as threshold secret solutions in [10] or [11] can cooperate with TAODV. These solutions provide secure way to issue public key certificates which can be used for the verification of digital signatures during the initialization of the newly joined nodes.

1) Routing Misbehavior Problem

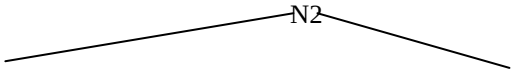
Misbehaving nodes at the routing level can be classified into two main categories [9]:

a) *Selfish node:* operates normally in the Route Discovery and the Route Maintenance phases of the AODV protocol. However, it does not perform the packet forwarding function for data packets unrelated to it self. The selfish node attempts to benefit from other nodes, but refuse to share its own resources.

b) *Malicious node:* acts to the detriment of the network by manipulating routing. Many routing protocols use hop count as a metric. A node can falsely claim a low hop count to a destination, enabling it to intercept traffic for that destination. Node identities are not authenticated, so a node can claim to be the destination of a route.

2) Trusted Route Discovery

When there is a source node S wants to send data to some destination node D and no route path is available. Then S will generate a TRREQ (trusted route request) message to discover the path the path to D. Any intermediate node M is supposed to have a route to the required destination node D. It will send the RREP (route reply) message to the S node. This route reply is sent only on the basis of trust combination among nodes. An example of trust combination is shown below:



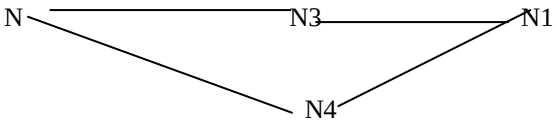


Figure1. Example for Trusted Routing Discovery

Here the trust combination is computed with the pair of nodes {NN2 with N1, NN3 with N1, and NN4 with N1} the greater trust combination pair will be selected.

Route Maintenance operation is same as in AODV.

V. CONCLUSIONS

We have compared the performance of on-demand routing aspects of DSR, AODV with their ATDSR and TAODV routing protocols. We have found that these protocols provide security and reliability in transmission of data with reasonable overheads. Further, these discovers multiple disjoints trusted paths for sending data traffic, however it chooses only one most trusted path. ATDSR and TAODV both the protocols adopted different approaches for route discovery and route maintenance. TAODV protocol avoids routing misbehaviour problems in terms of extra message and time delay where ATDSR manages the trust information locally with minimal overheads in finding trusted end-to-end routes. We believe in providing trusted routes are beneficial in network communications, particularly in mobile wireless networks where routes are disconnected frequently because of mobility and poor wireless link quality. One drawback of ATDSR scheme is its communication complexity because at each and every node trust value is computed. Simulation results [9] [13] [14] [15] of ATDSR and TAODV performs better than that of DSR and AODV.

REFERENCES

[1] Carlo Kopp, Defence Analyst and Consulting Engineer: "Ad Hoc Networking: Published in 'Systems'," June 1999, pp 33-40.

[2]D.B. Johnson and D.A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," In Mobile Cotnpting, edited by Tomasz lmielinski and Korth, Chapter 5, Kluwer Academic Publishers, 1996, pp. 153-181.

[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 Ann. Int'l Conf. Mobile Computing and Networking (MobiCom 2002), ACM Press, 2002, pp. 12–23.

[4] C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing in mobile wireless ad hoc networks," in Proc. 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA02), IEEE Press, 2002, pp. 3–13.

[5]Y. Hu, A. Perrig, and D. Johnson, " A secure on-demand routing protocol for ad hoc networks," in Proceedings of the 8th Ann. Int'l Conf. Mobile Computing and Networking (MobiCom 2002), ACM Press, 2002, pp. 12–23.

[6]D. B. Johnaon and D. A. Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks. Mobile Computing, pages 153-181, 1996.

[7] A. A. Pirzada , and C. McDonald, "Reliable routing in ad hoc networks using direct trust mechanisms," Advances in Ad Hoc and Sensor Networks Springer, 2006.

[8] K. Liu, and J. Deng," An acknowledgment-based approach for the detection of routing misbehavior in MANETs," IEEE Transactions On Mobile Computing, Vol. 6, No. 5, pp. 536-550, May 2007.

[9] K.. Fall and K. Varadhan, editors ,ns notes and documentation.
http://www.isi.edu/nsnam/ns/doc/index.html.

[10] S.Capkun, L. Buttyan, and J.P.Hubaux. Self-organized public-key management for mobile adhoc networks. In proceedings of ACM workshop on Wireless Security (WiSe '02), Atlanta, USA, September 2002.http://citesser.nj.nec.com/capkun02selforganized.html.

[11]J.Kong, P.Zefos, H.Luo, S.Lu and L.Zhang. Providing robust and ubiquitous security support for mobile adhoc networks. In proceedings of IEEE ICNP '01, 2001.

[12] Islam Tharwat A.Halim, Hossam M .A Fahmy, AYaman M. Bahaa EI-Din and H.EI Shafey "Agent based Trusted on Demand Routing Protocol for Mobile Adhoc Networks,6th international Conference communication on wireless networking and mobile 2010,pp, 1-8.

[13] X. Li, M. R. Lyu, and J. Liu, "A trust model based routing protocol for secure ad hoc networks," in Proceedings 2004 IEEE Aerospace Conference, Big Sky, Montana, U.S.A., March 6-13 2004.

[14] A. Gianni, and G. Di, "Analysis of simulation environments for mobile ad hoc networks", Dalle Molle Institute for Artificial Intelligence Vol. 1 No. (1): pages26-66, 2003

[15] A. A. Rahman, and S. Hailes, " A distributed trust model," in Proceedings of the ACM New Security Paradigms Workshop, Cumbria, UK ,1997, pp. 48-60.

[16] C. Perkins, E. Belding-Royer, and S. Das. Ad hoc on demand distance vector (aodv) routing. July 2003.