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. 3, Issue 4, April 2015

A Survey on the Secure Routing Protocols in MANETs

Ashwini S.N, P. Mangayarkarasi

M.Tech Student, Dept of ISE, The Oxford College of Engineering, Bangalore, India.

Assistant Professor, Department of ISE, The Oxford College of Engineering, Bangalore, India

ABSTRACT: Because of the characteristics, like dynamic network topology, limited bandwidth, and limited battery power, routing in a MANET becomes a challenging task compared to other conventional networks. Therefore research is targeting on development of efficient routing mechanisms. Many efficient routing protocols have been proposed for MANET, whose concept is based on the co-operation of each and every node that constitutes the network. The presence of misbehaving nodes, will lead to the vulnerabilities in the form of various kinds of attacks. This paper illustrates all the protocols for safe and secure routing in mobile ad-hoc networks. The objective is to know about various types of protocols which take different parameter as their prime consideration. But every protocol has the main aim of finding out the feasible path to route the packets providing security to the data being transmitted.

KEYWORDS: Trust based dynamic secure source routing(TDSSR), Route reply(RREP), route request(RREQ)

I.INTRODUCTION

The main feature of ad hoc technology is setting up a temporary network with a group of mobile nodes without any central infrastructure. It is a challenging task to support multimedia applications in IEEE 802.11 based ad hoc networks. In addition to mobility, a MANET can be constructed quickly at a low cost, as it does not rely on existing network infrastructure.Rapid development of Mobile Ad Hoc Networks (MANETs) has given rise to numerous wireless applications that can be used in a wide number of areas such as commerce, emergency services, military, education, and entertainment. MANETs features namely self-organizing and independent infrastructures, which make them an ideal choice for uses such as communication and information sharing.

Unlike the conventional or traditional network, MANETsare characterized by having a dynamic, continuously changing network topology due to mobility of nodes [1]. This feature makes it difficult to perform routing process in a MANET compared with a conventional wired network. In a dynamic network, it is difficult to use multimedia and other advanced applications without quality of-service (QoS) constraint. QoS shall be defined as the bundle of service primitives to be met while a network is in operation. In MANETs, designing a routing algorithm with given QoS constraint is hard because of the unavailability of accurate path information and it is difficult to keep up-to-date link information owing to its dynamic nature and reduction of energy levels in the nodes causes link breakage.

Currently many efficient routing protocolshave been proposed. These protocols are classified into two categories: reactive routing protocols and proactive routing protocols. In reactive routing protocols, such as the Ad hoc On Demand Distance Vector (AODV) protocol [2], nodes find routes only when required. In proactive routing protocols, such as the Optimized Link State Routing (OLSR) protocol [3], nodes obtain routes by periodic exchange of topology information. The routes are cached prior to their requirement.

Most of these routing protocols rely on cooperation between nodes which is due to the absence of a centralized administration. However, in an antagonistic environment, a malicious node can launch routing attacks to disrupt routing operations or denial-of-service (DoS) attacks to deny services to genuine nodes.

Trust [4] is defined as a degree of confidence about the behavior of other entities. The nodes participating in data exchange should be shielded by trust and reputation mechanisms or else they could be attacked which might end up with needless resource consumption of the entire mobile network. Attacks can be direct or indirect, i.e.,interlopers may take charge of good nodes which result in non-cooperation which leads to network devastation. Therefore, such

10.15680/ijircce.2015.0304165

nodes prone for compromise need to be acknowledged via trust and reputation mechanisms in advance so that the network is safe. The fact that , MANETs lack central administration, due to wireless set up and that will serve as thecrucial concern since it is easy for invaders to eavesdrop the packets, and tamper them.

II.PROTOCOLS

The objective of routing in a MANET is to determine the most recent topology of a continuously changing network to find a correct& feasible route to a definite node. Routing protocols in MANET are classified into two categories: reactive routing protocols (e.g., AODV) and proactive routing protocols (e.g., OLSR). In reactive routing protocols, nodes find paths only when they want to send data to the destination node whose route is unfamiliar. On the other hand, in proactive protocols, nodes periodically exchange topology information, so that nodes can obtain route information any time they want to send the data.In this section the different routing protocols are described.

AODV-AODV [5] comes under reactive routing protocol designed for mobile ad hoc network. In AODV, when source node S wants to send a data to a destination node D and does not have a route to D, it starts route discovery by broadcasting a route request (RREQ) to its neighbors. The neighbors who receive this RREQ rebroadcast the same RREQ to their immediate neighbors. This process is repeated unless and until the RREQ reaches the destination node D. On receiving the first inwards RREQ, the destination node sends a route reply (RREP) to the source node through the reverse path from where the RREQ arrived. If the same RREQ arrives later, it will be overlooked by the destination node. In addition, AODV enables intermediate nodes that have sufficiently fresh routes (with destination sequence number equal or greater than the one in the RREQ) to generate and send an RREP to the source node.

OLSR PROTOCOL- OLSR [6] is categorized as a proactive routing protocol, i.e., it is based on periodic exchange of topology information. The key concept of OLSR is the use of multipoint relay (MPR) to provide an effective flooding mechanism by reducing the number of transmissions required. In OLSR, each node selects its own MPR from its neighbors. Each MPR node maintains the list of nodes that were selected as an MPR; this list is called an MPR selector list. Only nodes selected as MPR nodes are responsible for advertising, as well as forwarding an MPR selector list advertised by other MPRs.

Routing Message in OLSR— Generally, in the OLSR protocol, two types of routing messages are used, namely, a HELLO message and a topology control (TC) message. A HELLO message is the message that is used for neighbor sensing and MPR selection. In OLSR, each node generates a HELLO message periodically. A node's HELLO message contains its own address and the list of its one-hop neighbors. By exchanging HELLO messages, each node can learn a complete topology up to two hops. HELLO messages are exchanged locally by neighbor nodes and are not forwarded further to other nodes. A TC message is the message that is used for route calculation. In OLSR, each MPR node advertises TC messages periodically. A TC message contains the list of the sender's MPR selector. In OLSR, only MPR nodes are responsible for forwarding TC messages. Upon receiving TC messages from all of the MPR nodes, each node can learn the partial network topology and can build a route to every node in the network.

MPR Selection-- For MPR selection, each node selects a set of its MPR nodes that can forward its routing messages. In OLSR, a node selects its MPR set that can reach all its two-hop neighbors. In case there are multiple choices, the minimum set is selected as an MPR set.

MULTI-PATH AND MESSAGE TRUST-BASED SECURE ROUTING-paths and if all the paths have trust less than the required trust, the message is divided, encrypted and then sent. This increases routing delay.

TRUST BASED SECURE ROUTING APPROACH-The agent based protocol is known as the trust based dynamic secure source routing (TDSSR) protocol. In this, an agent is installed in every node. An agent manifests four discrete characteristics namely intelligence, communication, autonomy and mobility. Intelligence is the capacity of the agent to acclimate itself and/or change its environment based on the availability of information. Communication is the property of an agent to interchange data with other agents existing in the same nodes or in other nodes. Through autonomy, the agent has the expert witness to control its actions and strategies without the necessity of human control.

Mobile agents have the ability to voyage easily across the network performing specific tasks. Overflowing the network with request messages isa useful tool for data searching in a fully distributedenvironment. However, since message transfer consumes both bandwidth and energy, trust and reputation management schemes that generate large amounts of traffic by flooding the network with request messages are not desirable in MANETs, as they are known for their bandwidth and energy constraints. Under these circumstances, a well-designed trusted routing protocol MANETs is a must. TDSSR selects the most trusted as well as the minimum hop count route from different possible routes with minimal overhead in terms of extra messages and time delay.

This protocol uses a multi-agent system (MAS) that consists of two types of agents that cooperate with each other to achieve the required task; specifically monitoring agent (MOA) and routing agent (ROA). MOA is responsible for monitoring its hosting node behaviour in the routing process and then computing and updating the trust value for this node. ROA is responsible for using the trust information and finding out the trust worthiest route and shortest route for a particular destination, as shown in the Fig1. The trust value is sent throughout the network with the routing information so as to avoid the extra messages, as shown in Fig2.To improve the security, the key exchange mechanism can be added.

In the proposed trusted routing mechanism, the Route Discovery includes three processes, (a)RREQ Delivery;(b)RREP Delivery; (c)Route Selection.

(a) RREQ Delivery

When the source node S wants to send the data to particular destination D, it checks in its cache, whether it already has the feasible path to the destination. If yes, it will proceed through that path. If it does not contain, it will start the route discovery process. The source node S will send RREQ packets to its immediate neighbors. The immediate neighbor accepts this RREQ only if it’s not a duplicate one.

(b) RREP Delivery

When the destination node D receives the RREQ packet, it checks the trust value of the route and also the time window. If it has reached within the stipulated time, it will accept the RREQ and send back the RREP through the same path through which it received RREQ.

(c) Route Selection

The source node, on the reception of RREP from the destination, will check the time window and the trust value of the path and decides whether that particular route is a safe route or not. If it’s a safe route, it will add it to its cache else blacklist it.

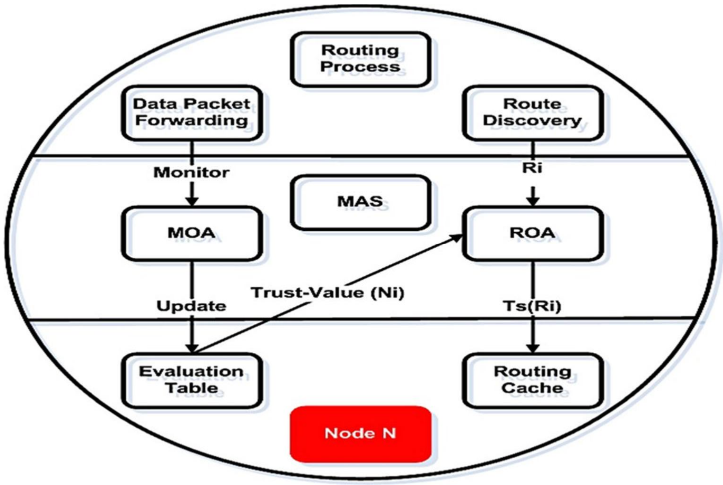

Fig1. Agent system

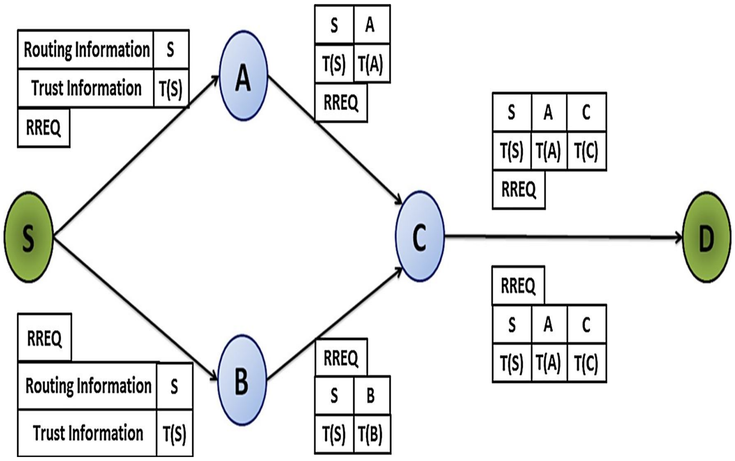

Fig2.Trust value propagation through RREQ packets

III. Conclusion

The routing protocol is a major concern for MANET's performance. This paper presents the survey of the protocols that are available for the routing purpose in mobile ad-hoc network. The advantages of every protocol can be diagnosed through the simulation in any of the simulator software with varying a variety of scenarios such as the number of malicious nodes, host density and movement rates. They can be studied and compared with each other through the same. The simulation results can show which protocol can effectively improve the energy efficiency and data delivery ratio in the presence of malicious nodes.

References

1. S. Ci et al., "Self-Regulating Network Utilization inMobile Ad-Hoc Wireless Networks," IEEE Trans. Vehic.Tech., vol. 55, no. 4, July 2006, pp. 1302–10.
2. C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc Ondemand Distance Vector (AODV) Routing," IETF RFC 3561, July 2003.

3. Th. Clausen et al., “Optimized Link State Routing Protocol,” IETF Internet draft, draft-ietf-manet-olsr-11.txt, July 2003.
4. V Manoj, A Mohammed, N Raghavendiran, R Vijayan, A novel security framework using trust and fuzzy logic in MANET. Intern J Distributed Parallel Systems 3, 1 (2012)
5. Th. Clausen et al., “Optimized Link State Routing Protocol,” IETF Internet draft, draft-ietf-manet-olsr-11.txt, July 2003.
6. Dhurandher, S. K. &Mehra, V. (2009). Multi-path and message trust-based secure routing in ad hoc networks. In Proceedings international conference advances in computing, control and telecomm. Technologies, Trivandrum, Kerala, pp. 189–194.
7. Subbaraj and Savarimuthu, Eigen Trust-based non-cooperative game modelassisting ACO look-ahead secure routing against selfishness EURASIP Journal on Wireless Communications and Networking 2014, 2014:78
8. Madhuri Gupta and Krishna KumarJoshi, “ An Innovative Approach to Detectthe Gray-Hole Attack in AODV based MANET”, International Journal of Computer Applications (0975 – 8887)Volume 84 – No 8, December 20113
9. Elhadi M. Shakshuki,Nan Kang, and Tarek R. Sheltami, “EAACK—A Secure Intrusion-Detection System for MANETs,” IEEE Trans. on industrial electronics, vol. 60, no. 3, march 2013

BIOGRAPHY

Ms. Ashwini S Na Student of Information Science and Engineering Department at The Oxford College of Engineering-Bangalore, affiliated to VTU pursuing M.Tech in Computer Networking and Engineering. She received her Bachelors of Engineering in Computer science and Engineering from Bapuji Institute of Engineering& Technology-Davangere affiliated to VTU. She is currently working as a research assistant under the guidance of **P.Mangayarkarasi.** Her research interests are Mobile ad-hoc networks and Information Security.

P.Mangayarkarasi has done her BSc in computer science from Saradha College of Engineering Affiliated to Anna University, MCA from Avinashilingham University, M.Tech in M.G.R University and currently pursuing her PhD under the field of software engineering in Visvesvaraya Technological University, Belgaum. She is currently working as the Assistant Professor in ISE Department of the Oxford college of Engineering. She has presented the paper on Dynamic Enterprises Architecture for one or more clouds in Journal of Engineering and IT Springer publications. She is guiding the M.Tech students in Network Engineering. She has around 10 years of teaching experience in leading educational Institutions in India. She has attended/conducted National and International level workshops, seminars and conferences.