ISSN 2229-5518

A Secure and Energy Enhanced Protocol for Routing in Mobile Ad-Hoc Networks

Deepthy Mathews, Shyama Sudarsan, S.Kannan and Dr.S.Karthik

Abstract- Mobile Ad hoc Network (MANET) is a network composed of wireless mobile nodes such as PDAs and laptops in such a way that, they are having the capability of wireless communication and which will form a network, without any fixed or existing infrastructure and centralized administration. In MANET, each and every node can act like an end system as well as a router. The mobile nodes can be connected by means of a standard Wi-Fi connection or another medium, where each device is free to move independently. They are also capable of moving randomly with the ability of changing their links to other devices frequently to which can make a connection. In this paper, we discuss the security mechanisms used in SAODV routing protocol and analyze its performance. It is clear that, the security mechanisms used in SAODV is expensive in terms of energy. Our paper deals with the idea of incorporating an energy efficient route discovery mechanism based on some energy threshold value in SAODV and thereby reducing it power consumption.

Keywords- Energy, Routing Protocols, Energy Efficient, Mobile ad hoc networks, Power Consumption, SAODV, Security attacks

1 INTRODUCTION

Mobile ad hoc network (MANET) is a new emerging technology which enables users to communicate without using any fixed or physical infrastructure. MANET is having self organizing and self adaptive capabilities. Each device in MANET is able to detect presence of other devices and then performs necessary set up to facilitate communication that can enable data sharing and other services. These types of networks are suitable for several types of applications like military operations, emergency and rescue operations, wireless mesh and sensor networks, collaborative and distributed computing etc. There are mainly three different types of MANET. They are,

- Vehicular Ad Hoc Networks (VANETs) which facilitate communication among vehicles and between vehicles roadside equipment.
- Intelligent Vehicular ad hoc networks (InVANETs) which eliminates most of the legacy PBX equipments and reduces the cost of installing a infrastructure for communication and maintenance cost once installed.
- Internet based Mobile ad hoc networks (iMANETs) those are the types of ad hoc networks which links mobile nodes with fixed. Internet-gateway nodes and thus normal ad hoc routing algorithms cannot be applied directly.

MANET is having the features like autonomous terminal, distributed operation, multi-hop routing, dynamic network topology, fluctuating link capacity and light weight terminals. Routing protocol, security, medium access scheme ,energy management [7], quality of service ,self organization, protocol multicasting, scalability are some of the challenges that are taken into account for designing a MANET. Dynamic behavior, link instability, node mobility and frequently changing topology of MANET makes the routing a core issue. An effective routing algorithm helps to extend the successful deployment of mobile ad hoc networks. And it finds a correct and efficient route between two nodes which will ensure correct and timely delivery of packets. A number of routing protocols has been proposed for MANETs [14],[2] which fall into two main categories, Proactive routing protocols and Reactive routing protocols. There is a new class of routing protocols called hybrid routing protocols, which makes use of the advantages of both proactive and reactive routing protocols [17]. In Proactive routing protocols, nodes continuously evaluate and update the routes. This is a table driven protocol which is efficient if the routes are used often but has large amount of overhead. In reactive routing protocol, nodes evaluate and update the routes only when they are needed and is efficient when routes are not used often. In hybrid routing, it uses the proactive routing mechanisms in some areas of the networks

Deepthy Mathews is currently pursuing masters degree program in Computer Science and Engineering in SNS College of Technology, India, PH-+91-422-2666264. E-mail: deepthiimathews@gmail.com

Shyama Sudarsan is currently pursuing masters degree program in Computer Science and Engineering in SNS College of Technology, India, PH-+91-422-2666264. E-mail: shyamasudarsancse@gmail.com

S. Kannan is an Assistant professor at the Department of Computer Science and Engineering, SNS College of Technology, India, PH-+91-422-2666264. E-mail: 6kannan6@gmail.com

Dr.S,Karthik is the Dean of Computer Science and Engineering, SNS College of Technology India, PH-+91-422-2666264.. E-mail:

and reactive routing mechanisms in the rest of the network.

MANET is highly exposed to security attacks in comparison to the traditional wired networks. There are five major goals [10] that need to be addressed for this type of networks in order to prevent malicious attacks. They are; Availability, Confidentiality, Integrity, Authentication, and Non-repudiation. The rest of this paper is organized as follows: we provide an overview of SAODV [9] and we propose the idea of power aware on demand routing with the objective to maximize the system life time of MANET, which may cause some changes in power requirement of SAODV routing protocol.

1.1 Security Attacks in MANET

The features of MANET like mobile nodes ,threats from compromised nodes within the network, dynamic topology, limited physical security, scalability and lack of centralized management makes it vulnerable to malicious attacks. In MANET there are two security aspects, one to protect the transmission of data and other is to make the routing protocol a secured one. There are a number of attacks which affects proper functioning of MANET. They can be classified as two main categories. Passive Attacks and Active Attacks [10],[15]. Passive attack is a type of attack which do not disrupt the proper operations in the network. The attackers will snoop or monitor the data exchanged in the network without altering it. Common examples [18] of passive attacks are eavesdropping, monitoring and traffic analysis. For this types of attacks, it is very difficult to detect them since they does not affect the normal functioning of the network. Active attacks are performed by some malicious nodes which modify the data stream or create a false stream of data. These nodes bear some energy cost in order to carry out their action. An active attack can be either external or internal. External attacks are carried out by some nodes that do not belong to the network being attacked. Whereas, internal attacks are from the compromised nodes which are a part of the network.

1.2 Mechanisms for Security

As MANETs offer new challenging security problems primarily due to their wireless network interface ,allowing easy eavesdropping and injection of messages, and due to their distributed infrastructure-less topology a number of security mechanisms are used [3] for preventing it from malicious attacks. Passive attacks can be prevented using encryption techniques. The mechanisms to avoid security issues are based on mainly two approaches:

- Prevention
- Detection and Reaction

Prevention based mechanisms will prevent the malicious nodes from actively initiating the attacks [11],[12]. They make use of encryption techniques for ensuring confidentiality, integrity, authentication and non-repudiation of routing information. Hu, Johnson and Perrig proposed a prevention mechanism using one-way hash chains called SEAD to avoid a malicious node from advertising falsely a better route or to prevent it from tampering the sequence number in the packets send by the source. They also proposed a prevention mechanism which uses the same one-way hash chain concept called ARIADNE. Security Aware Routing (SAR) protocol is an on-demand protocol which uses a symmetric key encryption method. Authenticated Routing for Ad-Hoc networks (ARAN) [16] which is an on demand routing protocol which uses asymmetric cryptography methods to detect and prevent all malicious nodes. It consists of a certification process followed by a route instantiation process to guarantee authentication. CONFIDANT is an extension to SAR protocol and it is a type of reputation based system. Secure Ad-hoc On-Demand Distance Vector Routing (SAODV) was proposed by Zapata and Asokan [12],[6], which is an extension of AODV protocol designed to protect only the routing messages and not the data packets. It uses two basic mechanisms, [13] digital signature and hash chains in order to make the routing messages like RREQ, RREP, RRER more secure.

2 EXISTING METHODOLOGY

SAODV addresses the problem of securing the routing messages in MANET. It is an extension of the AODV protocol [14] which is used to protect the route discovery mechanism. Working principle of SAODV [5], [8] is based on a key management subsystem that makes possible for each mobile node to obtain public keys from other nodes of the network. Then, each node is capable of securely verifying the association between the identity of a given ad hoc node and its public key thereby implementing the key management scheme. The SAODV can be implemented by using two key mechanisms:

2.1 SAODV Hash Chains

Hash chain mechanism is used to authenticate the hop count of RREQ and RREQ messages in such a way that allows every node that receives the messages to verify that the hop count has not been decremented by an attacker. Both the intermediate node and destination node performs this verification. This prevents an attack due to message tampering. A hash chain is formed by applying a one-way hash function repeatedly to a random number.

2.2 SAODV Digital Signature

Digital signatures [1] are the mechanisms used to protect the integrity of non-mutable data in RREQ and RREP messages. The only mutable field in the messages is the hop count. Using this mechanism, it signs everything except the hop count of AODV messages and hash from the SAODV extension. When a node receives a RREQ, it creates or updates a reverse route to that host only after verifying the signature. If the signature is verified, then it will store the route. In order to reply to a RREQ message, an intermediate

ISSN 2229-5518

node should fulfill the AODV's requirements and should have corresponding signature and old lifetime to put into the signature.

The RREP message will be send with a RREP signature extension. So that, whenever a node receives a RREP message from a host, it also will verify the signature before creating or updating a route to that particular host. If the signature is verified, it will store the route with the signature of RREP and lifetime.

3 PROPOSED METHODOLOGY

Energy management issues are very important in the context of ad hoc mobile wireless networks in general and sensor networks in particular. Energy needs to be optimally utilized. So that the nodes can perform their functionality satisfactorily. It is known that energy can be managed at various levels such as by using threshold values as given in [4]. For SAODV protocol, it uses some security mechanisms in the routing process which in turn causes the power reduction. In this paper, we propose energy management approach that can be used with SAODV protocol. The proposed idea deals with an on demand route discovery in terms of energy conservation. This mechanism does not require any type of energy awareness tables and thus reduces the routing overhead. The objective is to perform the SAODV routing mechanism in such a way that it avoids the low power nodes from the routing process. It considers the battery capacity of the network nodes as a crucial resource and thus extends the lifetime of each node and the entire network.

3.1 Energy Efficient Routing

The routing is to be done in such a way that it periodically checks the Remaining Battery Power (RBP) of nodes which falls under a given route and then compares it with a threshold energy value.

The energy efficient routing can be implemented in following steps;

a) The source node S broadcasts RREQ message containing the threshold value of energy, E_T

b) At neighbor node, if RBP> E_T a reply message is send and that node is selected for data transmission otherwise no any reply is sent from the node.

c) The source node checks for all the messages from its neighbors and the neighbor with highest residual energy and having a shortest active route to destination is selected for

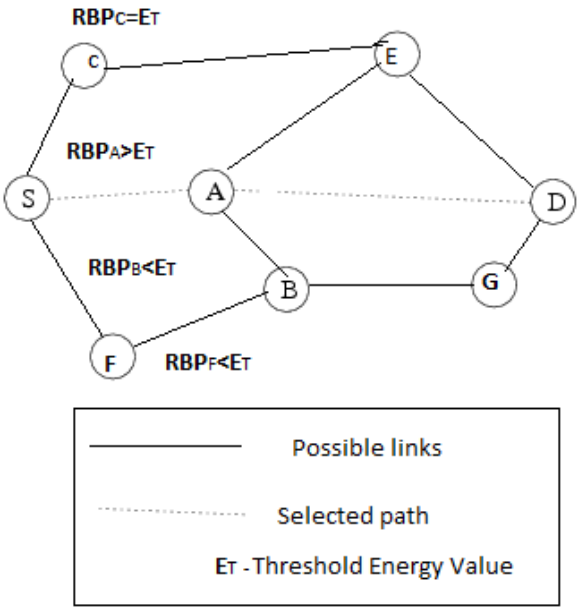

Fig. 1. Route discovery

forwarding the data and other nodes with are selected as alternate nodes in case of a link failure.

d) Source sends RREQ message to the selected node and it performs the security mechanisms .The node then forwards the same to the next node in the available active route.

e) The process is done for every node in the route and reverse route is saved. The destination node D then sends back the RREP on the saved path.

f) Source node S on receiving the RREP message ensures security of the path established and forwards the data over that path.

The mechanism of finding the optimal route between the source S and the destination D is shown in Fig 1. To find out the next node towards which data is to be send, the value of E_T is compared with the RBP value of each and every neighbors of the current node. Here for source S, its neighbor node A satisfies the requirement and thus is selected as the next hop.

4 RESULTS AND DISCUSSION

The SAODV protocol which is the security extension of AODV routing algorithm ,prevents the active external attacks by means of node authentication. SAODV outperforms the AODV routing in case of some parameters like higher packet delivery ratio in the presence of attackers and secure routing. But it has the drawbacks such as routing overhead, high processing power requirements etc. The routing overhead in SAODV is due to the security mechanism by using public key cryptography and the message size. This makes it an expensive routing protocol. Also SAODV has significant time delay in establishing routes. This is why, it requires a considerable amount of time for computing or verifying signatures and hashes at each node in the network. Thus it needs to reduce the routing overhead and its power requirements.

Table-driven routing protocols maintain a continuous view of the full topology of the network in each node, whereas on-demand protocols search for a route between a source and a destination when such a route is needed. Table-driven approaches introduce more overhead

compared to reactive ones. This is because whenever there are changes in the topology of the network, control messages are flooded in order to maintain a full knowledge of the network in each node. The main shortcoming of this criterion in terms of energy utilization is that the selection of routes in accordance with the min-hop principle does not protect nodes from being overused. When they run out of power, the network becomes partitioned and consequently some sessions is disconnected and causes the routing to fail. Since table-driven routing is inherently more energy-consuming compared to on-demand ones, focus of this work is to maximize network lifetime by an on demand energy-efficient routing. It works according to some threshold energy values which in comparison with the nodes RBP will return a best path for data transmission.

5 CONCLUSION

In this paper we discussed about mechanism of SAODV protocol which is a secured routing protocol for MANET. The major drawbacks of SAODV protocol such as overhead and power consumption affect it's the performance up to an extent. We proposed an idea to use a power aware routing concept in SAODV mechanism in order to solve its power consumption problem. The optimal route selection between source and destination using proper energy management may reduce amount of energy needed in SAODV routing mechanism and prolong the system life time by avoiding low power node for transmission. Our future work is to implement the enhanced SAODV protocol and simulate its performance using NS2.

REFERENCES

[1] Anil Suryavanshi and Dr. Poonam Sinha", Efficient Techniques for SAODV in mobile adhoc network," *Journal of Global Research in Computer Science* Volume 2, No. 8, August 2011.

[2] Asma Ahmed, A. Hanan, Shukor A. R., Izzeldin M.," Routing in Mobile Ad hoc Network," *IJCSNS International Journal of Computer Science and Network Security*, VOL.11 No.8, August 2011

[3] C.Sreedhar, Dr. S. Madhusudhana Verma , Prof. N. Kasiviswanath . "A Survey on Security Issues in Wireless Ad hoc Network Routing Protocols," *International Journal on Computer Science and Engineering*. Vol. 02, No. 02, 2010, 224-232

[4] Dr.A.Rajaram and J.Sugesh," Power Aware Routing for MANET Using On- demand Multipath Routing Protocol," *IJCSI International Journal of Computer Science Issues,* Vol. 8, Issue 4, No 2, July 2011

[5] Manel Guerrero. "Secure ad hoc on demand distance vector (SAODV) routing," *INTERNETDRAF draft-guerrero-manet- saodv-00.txt*. August 2001

[6] M. Guerrero Zapata and N. Asokan," Securing Ad Hoc Routing Protocols," *in Proc. ACM Workshop on Wireless Security (WiSe),* ACM Press, pp. 1-10, 2002.

[7] M. K. Marina and S. R. Das, "On- demand Multipath Distance Vector Routing in ad hoc networks," *ICNP, pp*. 14– 23, Nov 2001. " WMCSA, pp. 90– 100, Feb 1999.

[8] Preeti Sachan and Pabitra Mohan Khilar,"Securing AODV Routing Protocol in MANET Based on Cryptographic Authentication Mechanism," *International Journal of Network Security & Its Applications (IJNSA),* Vol.3, No.5, Sep 2011.

[9] Preeti Sachan and Pabitra Mohan Khilar ",Security Attacks and Solutions in MANET," *Proc. of Int. Conf. on Advances in Computer Engineering,* 2011.

[10] Priyanka Goyal, Sahil Batra and AjitSingh," A Literature Review of Security Attack in Mobile Ad-hoc networks," *International journal of Computer Applications,* Volume 9– No.12, November 2010.

[11] S. Yi, P. Naldurg, and R. Kravets, "Security-Aware Routing Protocol for Wireless Ad Hoc Networks," *Proc. of ACM MOBIHOC*, pp. 299-302, Oct. 001.

[12] Seung Yi, Prasad Naldurg, Robin Kravets ,"A security-aware routing protocol for wireless Ad Hoc networks. "

[13] Suman Deswal and Sukhbir Singh,"Implementation of Routing Security Aspects in AODV," *International Journal of Computer Theory and Engineering,* Vol. 2, No. 1 February, 2010.

[14] Sunil Taneja and Ashwani Kush, "A Survey of Routing mobile Ad Hoc Networks, "*International Journal of Innovation, Management and Technology,* Vol. 1, No. 3, August 2010.

[15] W. Stallings,"Cryptography and Network Security Principle and Practices", 3rd edition, Prentice Hall,2003

[16] Y. C. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," *IEEE Security and Privacy*, vol. 2, no. 3, pp.28-39, May-Jun 2004.

[17] S.Kannan, T.Kalaikumaran, S.Karthik and V.P Arunachalam", Ant colony Optimization for Routing in Mobile Ad-Hoc Networks," *International Journal of Soft Computing* 5(6) ,2010.

[18] S. Kannan, T. Maragatham, S.Karthik and V.P Arunachalam, "A Study of Attack Detection and Prevention Methods in Proactive and Reactive Routing Protocols," *International business Management* 5(3), 2011.