IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 4, Ver. VI (Jul – Aug. 2014), PP 46-51
www.iosrjournals.org

ASRMalNets: Acknowledgement Based Secure Routing Scheme for Malicious MANETs

Sreelakshmi S, Preetha K G
Department of Information Technology Rajagiri School of Engineering & Technology, Kochi

Abstract: *A mobile ad hoc network is a wireless commu- nication network, where communicating nodes are not within direct transmission range of each other. Since the radio links between the nodes break frequently, routing is a key issue in MANETs. The wide distribution of nodes makes MANETs vulnerable to malicious attacks. Hence huge researches are going on in this area. Efficient routing always conflicts with secure packet transmission. Both these issues are highly challenging in MANETs and should go by hand. The paper presents a technique to address this tradeoff. Malicious nodes interrupt the communication by dropping all the data packets. The paper is an Acknowledgment based Secure Routing Scheme in Malicious MANETs. According to this mechanism, the packet delivery is ensured even in the presence of malicious nodes. The main objective of this scheme is to achieve reliable data delivery in a malicious network. Performance of the proposed system is compared with the existing routing algorithm AODV using Network Simulator.*

Index Terms—Malicious networks, reliability, Mobile Ad-hoc
NETworks: *routing overhead, packet drop*

I. Introduction

Mobile ad hoc networks (MANET) have gained particular attention recently, as part of the next generation network technologies. These networks are usually constructed using mobile and wireless nodes with minimum or no central control or point of attachment such as a base station. These networks could be useful in a variety of applications from a one-off meeting network, to disaster, military applications, and entertainment industry.

MANETs can dynamically form a network to communicate each other. This does not require any fixed infrastructure. In many circumstances information exchange between mobile nodes cannot depend on any pre existing network infrastructure. Wireless ad hoc networks themselves are an independent, having wide area of research and applications, instead of just being a complement of the cellular system.

Due to the nature of MANETs like no proper boundary for communication; freedom of nodes to join the network; so on, they are highly hesitant. Some of the nodes may be compromised by the adversary and thus perform some malicious behaviors that are hard to detect. Lack of centralized machinery may cause some problems when there is a need to have such a centralized coordinator. Restricted power supply can cause some selfish problems and continuously changing scale of the network has set a limitation to the scalability of the protocols and services in the mobile ad hoc network. As a result, compared with the wired network, the mobile ad hoc network will need more robust security scheme to ensure its integrity.

The main objective is to overcome the security limitations of MANETs that it faces from its open, decentralized and dynamic nature. Owing to the unique characteristics of MANET, it is becoming more and more widely implemented in the industry. However, considering the fact that MANET is popular among critical mission applications, network security is of vital importance[1],[11]. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. ASRMalNets is an end to end acknowledgment based intrusion detection system that confirms reliability against receiver collision, power dissipation and false misbehavior problems.

The paper is structured as follows. In Section II, the background information related to malicious MANETs is introduced, including the MANET concept, features, current research status, and some of its applications. The proposed system is presented in detail in Section III. Section IV mainly discusses the simulation details with corresponding results. Finally, we summarize the paper by conclusions and future works in Section V and VI.

II. Current Research Directions

MANETs are highly vulnerable to different types of attacks. A brief description of different types of attacks that can occur in MANETs is given in [1],[2] and [19]. TableI gives a detailed idea about different types of active and passive attacks.

Many research efforts have been devoted to secure routing mechanism[8],[9],[10],[14]-[17]. Sead[3] is a secure and efficient distance vector routing protocol for mobile wireless ad hoc networks. Based on the Recommendation ITU- T M.3400, security management consisting of security administration, prevention and

detection of malicious nodes and containment and recovery is considered to be one of the major problems that MANETs are facing. This paper

Type	Layer	Attack
Active attack	Network layer	Spoofing Wormhole Blackhole Sinkhole Sybil Location disclosure Byzantine
	Multi-layer	Fabrication Modification Denial of Service Rushing
Passive attack	Datalink layer	Traffic analysis Monitoring
	Physical layer	Eavesdropping
	Multi-layer	Reply

Table I Attacks In Manets

Proposes a novel behavior detection algorithm combined with cryptography and digital certificates to satisfy prevention and detection, to securely manage the system.

Ad hoc networks supports a non-localised and fragmented networking structure that relies on communication of nodes for key network functionalities such as routing and medium access. In [4], a model based on the Sequential Probability Ratio Test was developed to characterize how nodes can differentiate between routes that include misbehaving nodes (infected routes) and routes that do not. An advantage of the model is that the number of observations required to evaluate a route need not be determined in advance, which is well-suited for the ad hoc networks with dynamic nature. A centralized and local approach is used to identify misbehaving systems on infected routes detected by the model. In [5], X.Y Zhang proposes a mechanism to detect black hole attacks in MANETs. It detects the attack before transmitting the packet. The destination sequence number of the route reply packet is used to identify the presence of attack.

Another key area of interest is intrusion detection system in MANETs. Many intrusion detection systems have been proposed in traditional wired networks, where all packets must go through switches, routers, or gateways. Hence, IDS can be added to and implemented in these devices easily. On the other hand, MANETs do not have such devices. Moreover, the medium is wide open, so both legitimate and malicious users can access it. Furthermore, there is no clear separation between normal and unusual activities in a mobile environment. In [6] and [7], the authors have made a detailed survey on IDS in MANETs. Since MANETs are dynamic in nature, any node can misbehave in the network. It can generate false routing information and hence make the network disturbed. Thus, the current IDS techniques on wired networks cannot be applied directly to MANETs. Many intrusion detection systems have been proposed to suit the characteristics of MANETs.

III. Proposed Methodology

ASRMalNets is an on demand routing scheme to ensure security and reliability in packet transmission. A modified version of Dijkshtras algorithm is used here to discover a position vector based route between each node and every other nodes. The observations show that it gives an optimal route be- tween every nodes. An acknowledgement based methodology is used to ensure reliability. The reception of acknowledgement confirms successful packet delivery to the destination node. Otherwise, a malicious path is suspected and another route to destination is discovered by reinitiating the routing algorithm. Then the packet is transmitted along this new route. The source node waits for the knowledgement. If there is no malicious nodes in this new route, the packet reaches the destination and then the destination node sends an acknowledgement back to the source node. It uses a bottom up approach as shown in Figure1.

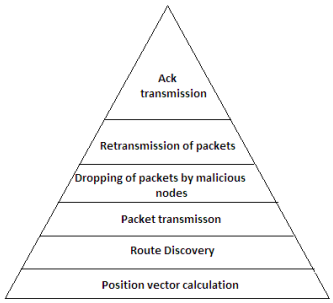

Fig. 1. Bottom up approach

The proposed system composes mainly three phases :

- Acknowledgement based packet transmission
- Detection of malicious nodes
- Retransmission of packets

A. Acknowledgement based packet transmission

The system uses position vector based routing i.e, the routing is based on the position vector of each node. Since this is an on-demand routing scheme, the source node finds the distance to other nodes, to find their neighbors, at the time when it has a packet to send. A modified version of Dijkshtras algorithm can be used. Then it checks which of its neighbors is closest to destination and considers that node as its next hop. Then this selected neighbor will take one of its neighbors that is closest to destination and considers that node as its next hop. This process continues till any node has its destination node as its neighbor. In this way the source finds a route to the destination node. Then it transmits the packet along this route. If this packet reaches the destination node, the destination node will send back an acknowledgement message back to the source node in the reverse direction. The reception of acknowledgement confirms succesfull transmission of packet as shown in Figure2. It also affirm that the nodes along this route as good nodes.

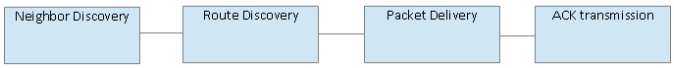

Fig. 2. Acknowledgement bassed packet transmission

B. Detection of malicious nodes

The reception of acknowledgements confirms successful packet transmission. If acknowledgement is not received within certain time, it suspects the presence of malicious nodes. Since malicious nodes in this type of attack has a packet dropping behavior, it drops each and every packet that it receives. Hence the destination does not receive the data packet. The source node hence, does not receive the acknowledgement.

C. Packet retransmission

Since non-reception of acknowledgement is treated as the presence of malicious nodes, and as reliability is the major concern of the system, there should be some way to find an alternate way to deliver the packet to destination. Therefore, the source node reinitiates the routing algorithm to find an optimal path to destination, by excluding the previous nodes along the suspected route. Then the data packet is transmitted along this route. If the packet reaches the destination, the destination node sends back an acknowledgement back to the source node. See Figure 3. This ensures reliability in any situation.

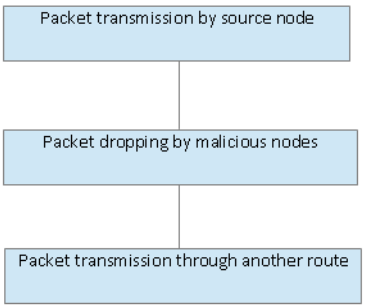

Fig. 3. Detection and retransmission

IV. Performance Evaluation

The description of the simulation scenarios and methodol- ogy is made in this section. The performance of the proposed system is compared with existing AODV[13] protocol, based on the packet delivery ratio and routing overhead.

A. Scenarios for Simulation

To better investigate the performance of ASRMalNets under different types of situations, the paper propose two scenario settings to simulate different types of routing behavior.

1) Malicious free networks: In case of non-malicious networks, ASRMalNets discovers the most optimal route to the destination node dynamically. The destination node sends back an acknowledgement when it receives the packet. This ensures the packet reception at the destination, to source.

2) Malicious networks: In certain situations, the path from the source to destination may contain some malicious nodes. In such scenarios, the data packet will not reach the destination. The non reception of acknowledgement within a threshold value, lets the source to know about the malicious nodes. Then the source finds an alternate path to destination. Hence reliability can be ensured in either cases.

B. Simulation Parameters

The simulation is conducted on Network Simulator, NS2.35[20] environment on Ubuntu 12.04. Assume a scenario of 20 nodes in a flat space of 600 x 600m . The simulation parameters are provided in Table II. The source node and destination node can be set dynamically. The physical layer,
802.11 MAC, Two ray ground propagation type and other wireless parameters are included in NS2. The moving speed of mobile node is limited to 20 m/s and a pause time of
1000 s. User Datagram Protocol traffic with constant bit rate is implemented with a packet size of 512 B.

In order to measure and compare the performances of the proposed scheme, it adopts the following two performance metrics :

1) Packet delivery ratio(PDR) : PDR defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node.
2) Normalized overhead : It can be defined as the ratio of routing packets to received packets by destination. It gives routing related information.

C. Simulation Results

The simulation results of PDR with AODV[12] is shown in Figure4. Since the packet drop is minimal in ASRMalNets, the PDR is high as shown. AODV does not ensure reliabilty too. Hence the scheme is better.

The routing overhead for both the protocols are same initially. In case of malicious MANETs, since to ensure reliability, the scheme discovers an alternate route, the overhead may vary depending upon the scenario. But the

Parameter	Value
Simulator	Network Simulator 2.35
Number of nodes	20
Topology	Random
Interface type	Phy/Wireless PHY
MAC type	802.11
Queue type	Droptail/Priority queue
Queue length	200 packets
Antenna type	Omni Antenna
Propagation type	Two Ray Ground
Transport agent	UDP
Application agent	CBR
Simulation time	50 seconds

TABLE II
SIMULATION PARAMETERS

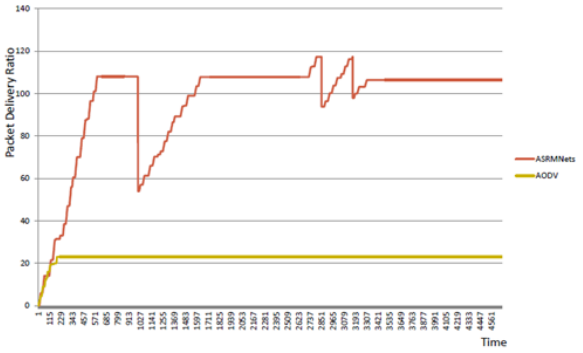

Fig. 4. PDR comparison

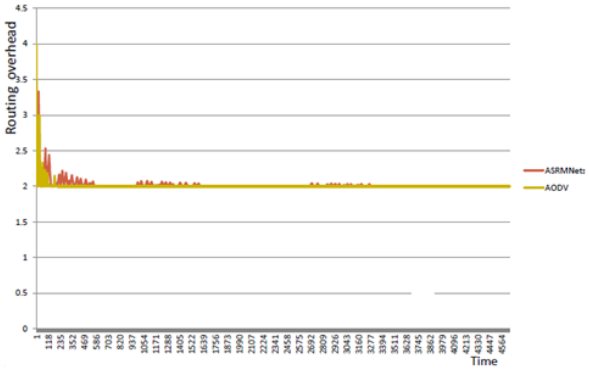

Fig. 5. Routing overhead

VI. Future Work

Research based on ASRMalNets can be extended in the following interesting ways.

1) ASRMalNets considers any type of packet drop as a misbehavior. This prevents a well behaving node from further transmission.

2) To ensure proper confidence and integrity, validation mechanisms can be made.

3) A malicious node can be recovered later, if possible.

This helps in exploiting the resources of the network at its maximum. Routing can be affected by many other factors like energy, mobility, and so on. Other factors can also be considered depending on the applications required

Effectiveness of reliable packet transmission makes this slight increase in overhead, negligible. The simulation results of normalized overhead is shown in Figure5.

V. Conclusion

MANETs are highly prone to different types of attacks. Packet delivery should be ensured even in the presence of malicious nodes. Thus it ensures security and reliability in packet transmission. An acknowledgement based methodology is used to guarantee packet delivery. If the source node does not receive any acknowledgement within a threshold time, then the source suspects a malicious path. Then it reinitiates a routing algorithm to find an alternative route to destination by excluding the malicious route. Thus it ensures packet transmission even in the presence of malicious nodes. A comparative study with the commonly used routing protocol AODV is made. The packet delivery ratio is higher for this system. In the case of routing overhead, both performs in

References

[1] Satyam Shrivastava, Sonali Jain, A Brief Introduction of Different type of Security Attacks found in Mobile Ad-hoc Network , ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003

[2] Sevil en, John A. Clark, Juan E. Tapiador, Security Threats in Mobile Ad Hoc Networks , Department of Computer Science, University of York, YO10 5DD, UK , August 2003

[3] Y. Hu, D. Johnson, and A. Perrig, SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks, in Proc. 4th IEEE Workshop Mobile Comput. Syst. Appl., 2002, pp. 313.

[4] N. Kang, E. Shakshuki, and T. Sheltami, Detecting misbehaving nodes in MANETs, i5. in Proc. 12th Int. Conf. iiWAS, Paris, France, Nov. 810, 2010, pp. 216222.

[5] Meenakshi Patel, Sanjay Sharma, Detection of malicious nodes in MANET using behavioral Approach , i5. in Proc. IEEE, 2012

[6] Tiranuch Anantvalee, Jie Wu, A Survey on Intrusion Detection in Mobile Ad Hoc Networks, i5.in Proc. Wireless/Mobile Network Security, Springer, 2006.

[7] K.R Valluvan, RajeshKumar G, A Comparative Study of Secure Intrusion- Detection Systems for Discovering Malicious Nodes on MANETs , i5.in International Journal of Computer Applications (0975 8887) Volume 67 No.18, April 2013

[8] Y. Hu, A. Perrig, and D. Johnson, ARIADNE: A secure on-demand routing protocol for ad hoc networks , in Proc. 8th ACM Int. Conf. MobiCom, Atlanta, GA, 2002, pp. 1223

[9] Gundeep Singh Bindra, Ashish Kapoor, Ashish Narang, Arjun Agrawal, Detection and Removal of Co-operative Blackhole and Grayhole Attacks in MANETs ,International Conference on System Engineering and Technology September 11-12, 2012

[10] N. Kang, E. Shakshuki, and T. Sheltami,EAACK-A Secure Intrusion- Detection System for MANETs , IEEE Journal on selected areas in communications, vol. 30, no. 2, february 2013.

[11] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester,An Overview of Mobile Ad Hoc Networks: Applications and Challenges, Department of Infor- mation Technology (INTEC), Ghent University IMEC vzw,2005.

[12] JG. Jayakumar and G. Gopinath,Ad hoc mobile wireless networks rout- ing protocolA review , J.Comput. Sci., vol. 3, no. 8, pp. 574582,2007.

[13] C.E. Perkins, and E.M. Royer,Ad-hoc On-demand Distance Vector Rout- ing , in Proceedings of the 2th IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, February 1999, pp.90-100.

[14] J. Lundberg,Routing security in ad hoc networks , in: Proceedings of the Helsinki University of Technology, HUT TML 2000

[15] Hongmei Deng, Wei Li, and Dharma P.Agrawal ,Routing Security in Wireless Ad Hoc Network , in IEEE Communications Magzine, vol. 40, Issue: 10, 2002

[16] P. Papadimitratos, and Z.J. Haas,Secure routing for mobile ad hoc networks, , SCS Communication Networks and Distributed Systems, Modeling and Simulation Conference (CNDS 2002), January 2002.

[17] V. Karpijoki,Security in ad hoc networks , in: Proceedings of the Helsinki University of Technology, Seminars on Network Security, 2000. [18] Nital Mistry, Devesh C Jinwala, Member, IAENG, and Mukesh Za- veri,Improving AODV Protocol against Black hole Attacks , IMECS2010

[19] S. Kannan, T. Kalaikumaran, S. Karthik and V. P. Arunachalam,A Review on Attack Prevention Methods in MANET , Journal of Modern Mathematics and Statistics 5(1) : 37-42, 2011

[20] NS-2.35 simulator, http://nsnam.org/