IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-5, Issue-12 E-ISSN: 2347-2693

Components for Designing of Secure Routing Protocol

S.S.Zalte[1*], V.R.Ghorpade[2]

[1*] Shivaji University, Kolhapur, India
[2] Bharti Vidyapeeth's College of Engineering, Kolhapur, India

[*]*Corresponding Author: sheetal.zaltegaikwad@*com, *Tel.: 9422785209*

Available online at: www.ijcseonline.org

Received: 03/Nov/2017, Revised: 15/Nov/2017, Accepted: 06/Dec/2017, Published: 31/Dec/2017

Abstract— In Mobile Ad-hoc Network(MANET) there are so many routing protocols are commenced. But no one will fulfill all security requirements. The crucial issue in MANET is Security due to the openness, infrastructure less and variable topology of MANET. In the broad dispersion of MANET, so many routing protocols are incorporated initially with the assumption that security must be retrofitted. Thus the routing protocols are more prone to various attacks with the risk of destruction of data. In this paper, we have discussed various components which will be required or helpful for designing of secure routing protocol in MANET.

Keywords—MANET, security, attacks, secure routing protocols, components

I. INTRODUCTION

From few years mobile ad hoc networks have gained major researcher's attention due to capabilities of infrastructure less and instant communication in many sensitive applications likes military, air force, business etc. applications. Many security protocols have been commenced to protect a transmission in mobile ad hoc networks [1] [2].

Mobile Ad-hoc Network is collection of different wireless mobile nodes which forms temporary network spontaneously as shown in Figure 1. They communicate with neighbors without any base station or centralized authority. Generally they have limited power and transmission range. So nodes in the network work in co-operative basis to forward packets. All the nodes in the network have freedom to move any where throughout the network irrespective of their neighbors. The vision for Mobile Ad-hoc Network includes data exchange frequently which facilitates routing, military application, e-commerce, business meetings etc. The traditional approach to network security involves cryptography which facilitates security primitive authentication, confidentiality, integrity and non-repudiation. But we believe this approach partially suitable for secure routing because some attacks other than the data modification like flooding network, Denial of service, replay and black hole attacks can be quite damaging the network. Further in MANET there is no guarantee that previous legitimate nodes will not be damaged the network. Hence, in MANET security relies upon most challenging issue of detecting and correcting malicious data. So while designing secure routing protocol for Mobile Ad-hoc Network, we have to taking care of not only data and route security but also we have to include intrusion detection system for attacks which are imposed by compromised nodes.

Figure 1. Mobile Ad-hoc Network

We have proposed general secure routing technique that allows detecting and preventing malicious nodes from routing that are the source of various attacks with high probability. The key components of secure routing protocols are secure neighbor discovery, cryptography and intrusion detection system.

Digital signatures-are employed to provide security to both routing traffic and data packets. A public key infrastructure that is RSA is adopted because of its beauty in distributing keys, achieving non-repudiation and authentication.

The aim of designing secure routing protocol is to provide security not only to data but also to route. This can be achieved with the help of security components which we have proposed in this paper. By using these components we can provide security to before routing begins and during routing process.

The rest of paper is arranged in the following way. In section 2, we will take short literature review, In section 3, we will refine the components of secure routing protocol. In section 4, we will present proposed frame work. We will conclude in section 5.

II. RELATED WORK

In paper [4] author proposed protocol which is based on aggregate signatures (merge several signatures in one) has been implemented in DSR protocol. For public key cryptography author has been used elliptic curve cryptography. Drawback is unable to detect node who has not signed in case of negative result.

To improve performance and security author have used the security of AODV will be based on one-way hash, two-way hash and digital signature in paper[5]. Here author generates two signatures. Intermediate nodes verify only first signature and accept packet and destination node verify second signature to check authenticity and integrity. The main advantage is that there is no need for certificate and key management scheme, less overhead of calculation, less battery consumption

Author proposed nested message authentication (NMAC) for hop-by-hop in paper [6]. To secure the routing packet in AODV and efficiently prevent most frequently occurred attacks such as black hole attacks, modifying routing information and impersonation attacks.

Here author used point to point authentication where nodes authenticate all type of routing control packets. The end to end authentication cannot be used for authenticating the packet like RERR messages where destination is not specified. This technique have very low overhead.

Author proposed modified form of AODV in [7] that is secured routing protocol (SecAODV). All nodes within MANET are distributed a certain IPv6 address value. In this scheme, the secured communication channel is established in between source and destination node depending upon the idea of Statistically Unique and Cryptographically Verifiable (SUCV) who confirms secured and secret binding between IPv6 address and key node

In paper[8] this scheme is unable to detect third node is malicious or not in four consecutive nodes third node is malicious or not in four consecutive nodes. The new enhance scheme keeps track information of ACK packets such as ACK for which, from where, ACK for whom etc. This characteristic of proposed scheme offers accurate detection of malicious node at third hop with first and second hop. Computation overhead is also very low.
Author construct a secure route discovery protocol (SRDP) in paper[9], which allows the source to find authenticated secure route to the destination by using either aggregated message authentication codes (MACs) or multi-signatures. This protocol is advantageous over the Ariadne in reducing computational overhead and offering non-repudiation.

Author proposed certificate based authority scheme for hop-by-hop authentication in [10]. Malicious nodes are detected by monitoring node's behaviour. Certificate allotment and revocation is done by Shamir's secrete sharing scheme. Each node monitors and evaluates the behaviour of its successors by itself, Certification revocation is done by calculating trust value of each node.

III. COMPONENTS OF SECURE ROUTING

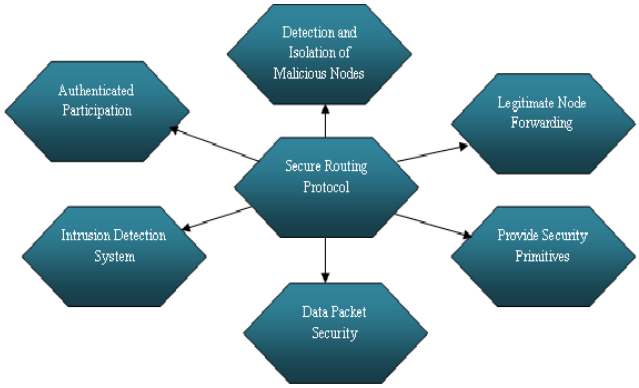

Figure 2. Components of Secure Routing Protocol.

To improve performance of routing protocol, it should be designed by using components which are mentioned in Figure 2.

2.1] Authentication:- It is the process of verification of someone or something is going to access their information. Furthermore, it is confirmation and validating their identity. While providing authentication to routing protocol we have to taking care of three important things that is limited battery power, memory limitations and bandwidth limitations. Mutual authentication is needed because each node must needed to know that other party must be authorized or legitimate node and is the part of mobile Ad-hoc network.

2.2] Intrusion detection system:-Design of intrusion detection system should able to detect malicious activity and provide proper solutions itself. There are so many intrusion prevention techniques such as authentication, encryption, access control and secure routing etc. The main goal of IDS is to detect malicious nodes and its activities and also encourages nodes to behave in a legitimate manner, i.e. to encourage good behaviour and to discourage malicious nodes from participating during communication.
2.3] Detection and isolation of malicious nodes:- As there is no physical line of defense, any node can easily participate

as legitimate node but in future, it may acts as malicious node and affect routine functions of routing. To detect such nodes and prevent them from routing is one of the biggest job.[11]

2.4] Only Legitimate node forwarding:-After detecting malicious nodes and their activities we realize which nodes are legitimate and which are malicious. So by changing flag of malicious nodes, we can prevent them from data forwarding for some time span. Only legitimate nodes can be allowed to participate in data communication.

2.5] Data Security:- To provide security to data packets cryptography is one of the most suitable technique. There are different types like asymmetric cryptography, symmetric cryptography, hashing etc. Each technique has its own pros and cons. By using encryption data can be scrambled and hide from the outside world. Even though malicious nodes capture data packets, they couldn't extract original data from encrypted text.

2.6] Security Primitives:-There are four security primitives Authentication, integrity, non-repudiation and confidentiality.

i] Authentication:-Receiver should be confident about received data packets should be coming from legitimate or authenticated user.

ii] Non-repudiation:-Non-repudiation services provide overwhelming evidence that a convinced event took place. A common example is sender cannot deny that the message is sent by him. Note that integrity is a prerequisite for non-repudiation.

iii] Confidentiality:-Encryption is used to provide confidentiality to information so other nodes cannot know what is the original information is.

iv] Integrity:-During routing contents of data packets should not changed when it reached to the destination. If any modification found in data packets that packet should be dropped. [12]

IV. PROPOSED FRAME WORK

In proposed method, to design secure routing protocol reactive routing protocols are the best for dynamic topology network than proactive routing protocol. In paper [13] author analyzed performance of AODV and DSDV protocol. He concluded that AODV's performance is the best considering its ability to maintain connection by periodic exchange of information. To achieve all components which are described in section III. We proposed to divide security mechanism in two parts

Security to route(pre-path security)-In this part authentication and access control can achieved by distributing public, private key pairs among nodes which are participated in network transmission. Here nodes which use fake public key or sending fake list of neighbours can be declared as malicious nodes. These malicious nodes are detected and prevented from the routing.

We can prevent data packets by using cryptography but for combat against active attacks like black hole, gray hole, DDOS and reply we have to use intrusion detection system.

Security to data packets (post-path security)-In this part data packets are encrypted with symmetric key algorithm and by using hashing and asymmetric algorithm digital signature can be implemented to achieve non-repudiation and confidentiality. Hashing is used for integrity.

V. CONCLUSION AND FUTURE SCOPE

Nodes in the MANET are unaware of network topology surrounding them and they have to discover it. As MANET is more prone to various attacks, active as well as passive attacks which brings catastrophic events in MANET as well as in networking. Secure routing protocol is not like packet should be reached at destination without modification but also from secured hands. Compromised nodes are internal nodes which are more dangerous to combat with such node's attack there should be strong mechanism like intrusion detection system. To thwart such attacks we have to design secure routing protocol by taking care of its security components which are mentioned in this paper.

ACKNOWLEDGMENT

I am gratified to my guide Vijay R. Ghorpade, who is always, supported and encourages me to do research work. I am also thankful to my supporters.

REFERENCES

[1] Hu Y., A.Perrig., "*A Survey of Secure Wireless Ad Hoc Routing*", IEEE Security & Privacy, 2004.

[2] Navneet Kumar, "*A Survey on Security in Mobile Ad-Hoc Network and Solutions*", International Journal of Computer Sciences and Engineering, Vol.3, Issue.7, pp.32-36, 2015.

[3] V.Bhargavi, M.Seetha, S.Viswanadharaju, " *A Trust Based Secure Routing Scheme for MANETS*", IEEE, pp-565-570, 2016.

[4] J.L. Tornos, J.J.Piles and J. L. Salazar," *ADSR: Authenticated DSR",* 2011 6th International Conference on Risks and Security of Internet and Systems (CRiSIS), IEEE,pp-1-8, 2011

[5] M.Pandya,A.K.Shrivastava.,"*Improvising Performance with Security of AODV Routing Protocol for MANETs*", IJCA, 78 , p1-1-7,2003.

[6] K. V. Arya, S. S. Rajput ," *Securing AODV Routing Protocol in MANET using NMAC with HBKS Technique*", 2014 International Conference on Signal Processing and Integrated Networks (SPIN), IEEE,pp-281-285, 2014

[7] A. Patwardhan, J. Parker, A. Joshi, M. Iorga and T. Karygiannis, "*Secure Routing and Intrusion Detection in Ad Hoc Networks,"* in Proc. of the 3rd IEEE – International conference on Pervasive Computing and Communications, March, pp. 191-199,2005.

[8] S. Soni, A. Parihar, " *Effective Intrusion Detection Scheme in Mobile Ad-Hoc Networks*", IJCA (0975 – 8887), Volume 135 – No.5, February 2016

[9] J. Kim, G. Tsudik,"SRDP: Secure route discovery for dynamic source routing in MANETs", elsevier,Ad Hoc Networks 7, pp-1097–1109,2009

[10] A.Rajaram ,S.Palaniswami, " *A High Certificate Authority Scheme for Authentication in Mobile Ad hoc Networks*", IJCSI, Vol. 7, Issue 4, No 5,pp-37-45, July 2010

[11] Anitha, J. Akilandeswari, " *Secured Message Transmission in Mobile AD HOC Networks through Identification and Removal of Byzantine Failures*", InterJRI Computer Science and Networking, Vol. 2, Issue 1,pp-14-18, August 2010

[12] N. Raza1, M. U. Aftab1, M. Q. Akbar2, O. Ashraf3, M. Irfan4, " *Mobile Ad-Hoc Networks Applications and Its Challenges*", Communications and Network, 8,pp- 131- 136,August 2016 .

[13] A Ambhaikar, D Mitra,R.Deshmukh, " *Performance of MANET Routing Protocol for Improving Scalability* ", Published in IJAEA, Jan 2011.

Authors Profile

Ms Sheetal S. Zalte pursed Bachelor of Computer Science from Pune University, India in year 2002 and Master of Computer Science from pune, India, in year 2004. She is currently pursuing her Ph.D. in Mobile Adhoc Network. She has 9 years teaching experience in computer science.She has published research papers in reputed international journals and conferences including IEEE and it's also available online.

Vijay Ghorpade pursed B.E. degree and M.E. degrees in Computer Science and Engineering from Marathwada University, Aurangabad, and Shivaji University, Kolhapur, India, in 1990 and 2001 respectively. In 2008, he earned his PhD degree at SGGSIET, Nanded, India. Presently he is working as Principal at Bharti Vidyapeeth's College of Engineering, Kolhapur, India. His research interests include network security and ad hoc network. He has published more than 20 research papers in reputed international journals including IEEE.

