A Survey on An efficient secure routing scheme for MANET

[1]Dipika Kolipatel, [2]Krunal Panchal

[1] Student ,Information Technology, L.J.I.E.T, Gujarat, India
[2] Assistant Professor, Computer engineering, L.J.I.E.T, Gujarat, India

ABSTRACT

Mobile Ad hoc NETwork (MANET) is a collection of self-organizing mobile nodes without any help of centralized administration or established infrastructure. Due to this characteristic, MANETs are particularly vulnerable to various security threats. Different routing protocols are developed for communication in MANET. Moreover in MANETs security is the major concern because it widely used in applications such as communication and data sharing .Secure routing protocols are developed as one of security mechanisms. This paper attempts to provide a comprehensive overview of secure routing protocols and some other techniques to secure, routing process in MANET.

Keyword : *MANET; Security attacks; secure routing protocol; Malicious node detection techniques*

1. INTRODUCTION

1.1 MANET

A Mobile Ad Hoc Network (MANET)[1] is a continuously self configuring, infrastructure-less network of mobile devices connected without wires. Ad Hoc is Latin & means "for this purpose" Each device in a MANET is free to move independently in any direction and will change its links to other devices frequently.

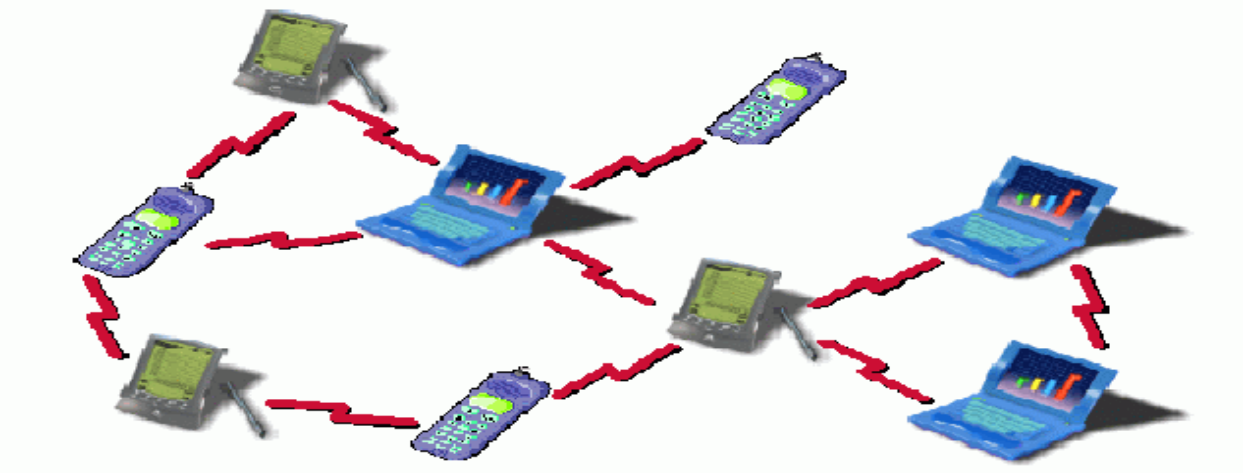

Fig -1: MANET[2]

MANET[3] architecture is not having centralized network, and therefore nodes are moving freely and randomly. Due to MANET decentralized network it is self-configuring and self-maintaining. Due to such features of MANETs, they are used in application such as military conflict, human induced disasters and medical emergency recovery. As there is decentralized architecture in MANET, enforcing policy is difficult because they lack

infrastructure. Securing wireless ad-hoc networks[4] is a highly challenging issue. Security of communication in MANET is important for secure transmission of information. Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to attacks than wired network there are a number of attacks that affect MANET.

1.2 ATTACKS IN MANET

Due to characteristics of mobile ad-hoc networks[5],MANETs are more vulnerable to be attacked than wired networks. We can distinguish two principal categories of attacks: passive and active attacks. A passive attack does not disrupt the operation of the protocol, but attempts to listen to valuable information in the traffic. Instead, an active attack disrupts the operation of the protocol in order to degrade the network performance, gain unauthorized access, and restrict availability. Several well-known routing attacks[5] are like Passive Eavesdropping Attack, Routing Data Manipulation Attack, Replay Attack, Black Hole Attack, Flooding Attack, Rushing Attack, Tunnelling/Wormhole Attack etc affect MANET.

1.3 SECURE ROUTING PROTOCOL

Routing[10] is the communication between two nodes in a network. Routing is the process of forwarding packet towards its destination using most efficient path. Routing efficiency is measured in terms of Number of intermediate nodes, delay ,throughput, security, etc. Routing protocols are divided into reactive, proactive and hybrid. The primary objective of an ad-hoc network routing protocol[6] is the correct and efficient route establishment between a pair of nodes so that messages may be delivered reliably and in a timely manner. If routing can be misdirected, the entire network can be compromised. Thus, secured routing plays an important role in the security of the mobile ad hoc network.

Secure Routing Protocol (SRP)[6,7], Security-aware Ad hoc Routing (SAR) protocol, Authenticated Routing for Ad hoc Networks (ARAN), Secure Efficient Ad hoc Distance vector (SEAD), The Secure Ad hoc On-demand Distance Vector protocol (SAODV), Secure Link State Routing Protocol (SLSP)[6], Ariadne etc are some secure routing protocols that use some cryptographic techniques for preventing MANET from different attack.

Table-1. Summary Report for Secure Routing Protocols[7]

S.No	Protocols	Attacks	Mechanisms	Advantages	Disadvantages
1.	SDSDV	Hostile attacks and Protects on the sequence numbers and metrics	Uses hash chain solution. SDSDV postulates that each node creates two hash chains in relation to each node in the network, including itself, with one used for guarding against the decreasing metric attack and the other for against increasing metric attack.	SDSDV can provide a complete protection on the routing messages ,the hash chain approach uses Symmetric cryptography which has lower computation complexity compared to asymmetric cryptograph.	1)The increased overhead in SDSDV may cause some degree of congestion in the network. 2)The longer routing delay may cause more packets to be dropped. 3)Deterioration of SDSDV due to the overhead is not significant. 4)SDSDV may not suitable for a large ad-hoc network.
2	SEAR	1)Trace back attacks 2)traffic jamming attacks	Consists two methods for packet forwarding: shortest path forwarding	SEAR can provide excellent balance between routing efficiency and energy	Increased overhead since the a mixture of the random walking and the shortest path

		3)minimize possibility for DOS attacks	based on the geographical information, and random forwarding, which is used to create routing unpredictability for source privacy and jamming prevention.	consumption while preventing routing trace back attacks and malicious traffic jamming attacks.	routing.
3	Ariadne	1)Fabrication attacks 2)Packetdropping attack 3)Selfish misbehavior 4)Black hole attack	1)Message Authentication Code 2)Digital signature	1)Ariadne is DSR based protocol that overcomes this attack. 2)The first implementation of this protocol is TESLA and another implementation is Massage Authentication code.	1)The major issue is to make sure the data is secure and arrives safely without any attacks from the adversary. 2)most of the solutions are more focus on data packets and not directly applicable to control packets.
4	ENDAIRA	1)DOS 2)Hackers 3)Selfish misbehaviour	Cryptographic signature	Definition of routing security, to model the operation of a given routing protocol in the presence of adversary, and prove that the protocol is secure.	1)more route discoveries, more latency due to cryptography computation before sending the data packets. 2)The most important issue is monitoring procedures.
5	ARAN	1)route disruption, 2)route diversion, 3)creation of incorrect routing state 4)spoofing attacks	Digital signature	The messages use certificate revocation for detecting expired public keys.	it is actually disconnected from the rest of the network
6	SAODV	1)resilience to attack from malicious nodes 2)Selfish attacks	1) non invertible hash functions and public key cryptography. 2) SAODV uses a double signature mechanisms to allow an intermediate node to reply to their request.	SAODV resulted a good compromise between reactive information exchange and security mechanisms based on an on-demand authentication mechanisms and control overhead.	The resource consumption of each node for the cryptographic operations would become very expensive.

2. RELATED WORK

- Limitations of MANET are limited battery power and limited bandwidth.Moreover, MANET is vulnerable to various security attacks which degrade the security and performance,So to improve network performance

different detection techniques[8] like watchdog, TWOACK system, AACK system, EAACK etc are proposed. This technique has also some limitation to solve it SPSS is introduced.

- Game theoretic[9] concept is useful to detect malicious node. Using game theory we can find out the effects of selfish nodes and malicious nodes on the network. Using payoff matrix we can prove that every node in the network will be benefitted by behaving cooperatively.

- Anonymous routing protocols[10] a r e used by MANETs that hi de s the identity of nodes as well as routes from outside observers. In MANETs anonymity means identity and location anonymity of data sources and destinations a s well as route anonymity. However existing anonymous routing protocols have significantly high cost, which worsens the resource constraint problem in MANETs, SHARP is proposed.

- Some secure routing protocols are introduced for securing MANET routing. Most of the existing secure routing protocols target to evade specific type of attacks or malicious behaviour of the nodes or networks. So, novel secure way routing protocol SWR[11] is proposed for securing the dynamic way routes in MANET.

- Routing techniques[12] like flooding, Epidemic routing, SNW etc are avilable for ICMN, these routing techniques it is impossible to provide secure communication. To make it possible new scheme called Privacy preserving ant routing protocol using ant colony optimization technique is introduced.

2.1 LITERATURE REVIEW

- Sachin D. Ubarhande,Dharmpal D. Doye, Prakash S.Nalwade [8] proposes a distributed delegation-based scheme, namely, a secure path selection scheme. The proposed scheme identifies and allows only trusted nodes to become part of active path. The SPSS scheme establishes a secure path from source to destination in presence of attackers.[1]

- Debjit Das, Koushik Majumder, Anurag Dasgupta[9] propose A Game-Theory Based Secure Routing Mechanism in Mobile Ad Hoc Network. Here, based on Packet Forward Rate (PFR) and Route Density Factor (RDF), a new scheme based on game theory has been developed that will detect selfish nodes and avoid malicious nodes of the system for packet transmission. During data transmission if any node of the selected path moves out of the radio range, then an alternate backup route will be formed from that position so that data transmission never stops. So, this scheme guarantees secure routing and constructs alternate backup route for guaranteed packet transmission.

- Remya S, Lakshmi K S[10] propose Secured Hierarchical Anonymous Routing Protocol (SHARP) based on cluster routing. SHARP offers anonymity to source, destination, and routes. Anonymous routing protocols a r e used by MANETs that hi de s the identity of nodes as well as routes from outside observers. In MANETs anonymity means identity and location anonymity of data sources and destinations a s well as route anonymity

- Jarupula Rajeshwar,Gugulotu Narsimha[11] propose Secure way routing protocol for mobile ad hoc network, which secure the routing mechanism from both the internal and the external attacks. Most of the existing secure routing protocols target to evade specific type of attacks or malicious behaviour of the nodes or networks. This paper propose a novel secure way routing protocol for securing the dynamic way routes in MANET. It provides a unique session key for each route to secure the data communication. Moreover, it authenticates the data packets using asymmetric cryptography and secures the routing field message using two-way asymmetric cryptography.

- S. Ramesh[12] propose An Efficient Secure Routing for Intermittently Connected Mobile Networks.The paper exhibits the efficient secure routing by PPARP which shows a higher level of security in ICMN. Secure communication in the network is made possible by certain authentication series as ICMN is known

for its higher delays. A peculiar routing protocol called Privacy Preserving Ant Routing Protocol (PPARP) which is a fusion of ACO with authentication series promises us an expected security.

2.2 COMPARATIVE TABLE

Table -2: Comparative Table

Sr No.	Paper Title	Method Used	Advantage	Disadvantage
1	A Secure Path Selection Scheme for Mobile Ad Hoc Network	SPSS	Perform well as compared to EAACK	Optimization is not done.
2	A Game-Theory Based Secure Routing Mechanism in Mobile Ad Hoc Network	game theory	guarantees secure routing & ensures minimum amount of idle time .	Time complexity
3	SHARP : Secured Hierarchical Anonymous Routing Protocol for MANETs	Cryptographic techniques, RSA	SHARP offers anonymity to source, destination, and routes and achieves better anonymity protection compared to other anonymous routing protocols.	In the formation of cluster there is no strategy of cluster head so it may degrade performance of network.
4	Secure way routing protocol for mobile ad hoc network	Secure way routing (SWR) protocol	SWR can detect internal and external both attacks and Provide better security than AODV, SAODV, SRAODV and ARAN	Cannot handle link failure and repair the proces.
5	An Efficient Secure Routing for Intermittently Connected Mobile Networks	Privacy Preserving Ant Routing Protocol	PPARP act as a better protocol for data delivery towards the terminus without affecting the performance, provide higher level of security	When number of nodes increase it degrades network performance.

3. CONCLUSION

Mobile ad-hoc network have been increase their vulnerability to attacks. This paper have discussed and presented various issues such as security attacks and threats can cause vulnerability in MANETs. It has been analyzed security mechanisms of various existing routing protocols in Mantes, which implements against various types of external attacks detect malicious behaviour and provide a safer environment, with the secure routing can be successful authenticated and the malicious nodes can be identified. number of challenges remain in the area of securing wireless ad hoc networks. The secure routing problem in such networks isn't well modelled. Although researchers have designed efficient security routing, optimistic approaches can provide a better tradeoffs between security and performance.

4. REFERENCES

[1] Jai Shree Mehta, Shilpa Nupur,Swati Gupta."An Overview of MANET: Concepts, Architecture & Issues",International Journal of Research in Management, Science & Technology (E-ISSN: 2321-3264),Vol. 3, No. 2, April 2015(pp:98-101)

[2] Dongbin Wang, Mingzeng Hu and Hui Zhi,"A survey of secure routing in ad hoc networks",The Ninth International Conference on Web-Age Information Management,978-0-7695-3185-4/08 $25.00 © 2008 IEEE(pp:482-486) DOI 10.1109/WAIM.2008.79.

[3] Poonam Joshi, Pooja Nande, Ashwini Pawar, Pooja Shinde, Rupali,"EAACK- A Secure Intrusion Detection and Prevention System for MANETs",International Conference on Pervasive Computing (ICPC),978-1-4799-6272-3/15/$31.00(c)2015 IEEE.

[4] Mr. L Raja,Capt. Dr. S Santhosh Baboo,"An Overview of MANET: Applications, Attacks and Challenges",International Journal of Computer Science and Mobile Computing, Vol.3 Issue.1, January- 2014, pg. 408-417.

[5] Houda Moudni1, Mohamed Er-rouidi1,Hicham Mouncif2, Benachir El Hadadi2,"Secure Routing Protocols for Mobile Ad Hoc Networks",978-1-4673-7689-1/16/$31.00 ©2016 IEEE.

[6] CHARU WAHI1 & SANJAY KUMAR SONBHADRA2,"SURVEY OF SECURITY ISSUES IN ROUTING OF MOBILE AD HOC NETWORKS",International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC) ISSN(P): 2250-1568; ISSN(E): 2278-9448 Vol. 4, Issue 1, Feb 2014, 71-78

[7] Dr. V.Umadevi Chezhian1 S.Geetha2, G.Geetharamani,"Survey on Secure Routing Protocols in MANET",International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 7, July 2014,pp-7609-7611

[8] Sachin D. Ubarhande,Dharmpal D. Doye, Prakash S. Nalwade(2017)." A Secure Path Selection Scheme for Mobile Ad Hoc Network. " Wireless Personal Communication ,Springer, DOI 10.1007/s11277-017-4597-1.

[9] Debjit Das, Koushik Majumder, Anurag Dasgupta(2016)." A Game-Theory Based Secure Routing Mechanism in Mobile Ad Hoc Network ". International Conference on Computing, Communication and Automation (ICCCA2016) ,(pp-437-472). IEEE.

[10] Remya S, Lakshmi K S(2015)." SHARP : Secured Hierarchical Anonymous Routing Protocol for MANETs ". 2015 International Conference on Computer Communication and Informatics (ICCCI), 978-1-4799-6805-3/15/$31.00 @2015 IEEE.

[11] Jarupula Rajeshwar,Gugulotu Narsimha(2015)." Secure way routing protocol for mobile ad hoc network". Wireless network, by SPRINGER, DOI 10.1007/s11276-015-1161-3.

[12] S. Ramesh(2016)." An Efficient Secure Routing for Intermittently Connected Mobile Networks " Wireless Personal Communication DOI 10.1007/s11277-016-3885-5.