ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

A SURVEY ON SECURITY SCHEMES FOR MANET

V. Pazhanisamy, J.Nithyapriya
Head,Dept.of CS and Engineering,Research scholar,
Alagappa University,
Karaikudi,Tamilnadu,India
Vpazhanisamy@yahoo.co.in
nihyapriyajj@gmail.com

Abstract: **Mobile Adhoc Network called MANET is proven to be the top research area with the focuses on security, performance, energy and so on. Being a network which is able to connect multiple nodes and networks with any large distance security becomes the biggest concern because the information travels through many unknown nodes and multiple paths. There are number of security challenges for MANETs .Since the nodes always keep moving and having no central administrator, rather than giving flexible topology it is more prone to attacks. This paper reviews various security attacks and various security techniques so far provided for MANET and analyzes their merits and drawbacks.**

Keywords:MANET,SATEM

I. INTRODUCTION

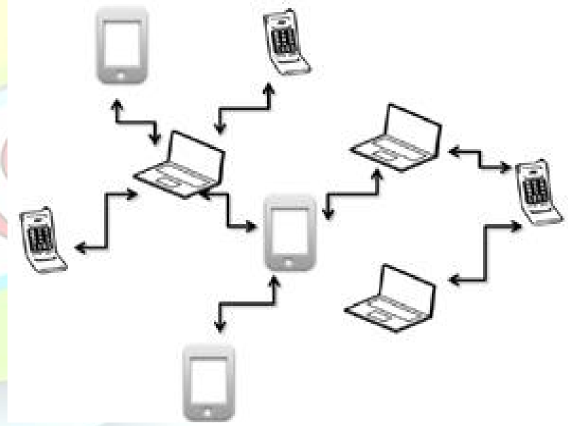
Wireless nodes network among themselves even when the access to the internet is unavailable. Right from instant conferencing between users of personal computers to emergency and military services that performs during harshest conditions adhoc helps. Adhoc networks have a unique set of challenges.

[1]The dynamic changing topology consumes much power and thus it limits the cryptographic measures.

[2]Lack of central administration causes passive eavesdropping, impersonation, DoS, message replay and message distortion.

[3]Mobile nodes are easy to compromise for security like unauthorized listening, modification and attempt to masquerade on the wireless communication channel as one of the legitimate node in the network.

[4]Routing appears to be complex for MANETs.



II. VARIOUS SECURITY SCHEMES SUGGESTED FOR MANET

1. Immune Inspired Approach For Securing Manet[1]

The main issues of Manets are bandwidth, scalability, and complexity. One of the most outstanding characteristic of mobile ad hoc networks is scarce and variable bandwidth. It is essential that any system must impose a very little traffic overhead on the network. On the other hand it is necessary to achieve reliable scalability to gather and analyze the high-volume of data correctly from distributed hosts that have a high mobility nature. In the environment of huge number of mobile nodes the malicious node has to be detected and they do it with the help of maintaining different profiles .

- **Detectors profile:** Responsible for distinguishing the nonself to be eliminated.
- **Non self profile:** Contains the events that harm the system. Assures the proper treatment in the future
- **Genes profile:** Contains necessary and frequently occurring events for the connection establishment, similar to self cells in the immune system.

2. Novel Security Scheme[2]

This scheme detects malicious node using the techniques hashing and masking. This scheme suggests sending the secret code from the sender to the receiver through multiple paths rather than single path. Multiple paths are selected with many intermediate nodes between the sender and the receiver. The exact code is not sent but shares, a portion of data. The receiver extracts the original data through masks suggested by the sender. The following are the drawbacks of this scheme.

Drawbacks of NSS

- No time frame is not
- Threshold is unknown to the receiver
- No facility of detecting malicious route

3. Enhanced Novel Security Scheme: ENSS[3]

ENSS proposes an enhanced scheme for more reliability of the novel scheme. ENSS proposes a mechanism to protect integrity of the data. Core concept of message sending using shared cryptography remains unchanged.

The following modifications are suggested by ENSS:

- Each path is assigned a number that will be helpful in deciding malicious route.
- The unique number assigned for each share of same message helps receiver to differentiate different message from same sender.
- Since receiver gets value of the threshold, receiver will get exact idea of the threshold number of shares.
- Hash value of the message protects the integrity of the secret data.

4. Secured Scheme For Ad Hoc Networks Using Encryption As A Tool[4]

An encryption algorithm at the source site will encrypted the entire packet. The packet will be encrypted with the help of a particular key. The key has 8 distinct blocks. With the help of these blocks encryption is performed. In case of successful encryption it transmits the packet.

5. SPAWN: A Secure Privacy-Preserving Architecture In Wireless Mobile Ad Hoc Networks[5]

SPAWN architecture includes the concept of observer obscurity to provide privacy and security for the genuine nodes and to exclude misbehaving nodes in the network. A misbehaving node is categorized as outlier or malicious. A misbehaving node is one who drops the data packets instead of forwarding and malicious is one who does not send cooperation message, upon receiving a caution. These nodes are excluded in two ways: firstly, a user is declared as outlier if the overall trust is less than the threshold. Secondly, a user is revealed as malicious if it does not send a cooperation message upon receiving a caution. Energy consumption is high when the number of nodes exceeds a certain level.

6. False Node Detection Algorithm in Cluster Based MANET[6]

The logic behind clustering is to collect the network nodes into a number of overlapping clusters. Clustering makes possible a hierarchical routing in which paths are recorded between clusters instead of between nodes. Nodes in network must cooperate with the other nodes. This algorithm detects the false node, which do not or partially cooperate. This algorithm detects false nodes only between clusters not inside a cluster.

7. Removal Of Selective Black Hole Attack In MANET By AODV Protocol[7]

A selective black hole attack on MANET refers to an attack by a malicious node, which forcibly acquires the route from source to a destination by the falsification of sequence number and hop count of the routing message. As selective black hole perform a selective black hole attack or perform as a normal node. This paper proposes a method of activating the promiscuous mode and hence further data packet loss is prevented. Finally, the performance of the nodes after the inclusion of promiscuous mode is analyzed. This scheme does not detect the initial packet loss.

8. Secure Communication in Mobile Ad-Hoc Network Using SATEM [8]

SATEM, Service-aware Trusted Execution Monitor to build the trusted policy enforcing mechanism. SATEM is composed of a trusted agent in the OS kernel of the service platform and a trust evaluator on the user platform. The service provider performs the attestation of the OS kernel including the trusted agent through a trusted boot process using the TPM specified by the Trusted Computing Group (TCG).Subsequently, the trusted agent takes advantage of the service execution context to only verify the integrity of the code loaded dynamically by the service. SATEM is developed for establishing a trusted connection. Each node in the network should have the trusted platform. So they can establish a trusted connection between nodes. A major limitation about this scheme is if false key is generated file transaction cannot be done.

III. ANALYSIS TABLE

SNo	Technique	Year	Drawback
1	Immune Inspired Approach	2009	Complex and time consuming
2	Novel Security Scheme	2011	Time consuming, Unable to detect malicious node
3	Enhanced Novel Security Scheme: ENSS	2012	Not energy efficient
4	Secured Scheme For Manet Using Encryption As A Tool	2013	Does not support scalability
5	A Secure Privacy-Preserving Architecture In Manet	2013	Energy consumption is high when the number of nodes increases.
6	False Node Detection Algorithm	2014	Does not detect false node inside a cluster
7	Removal Of Selective Black Hole By AODV Protocol	2014	Does not detect the initial packet loss.
8	Secure Communication in Mobile Ad-Hoc Network Using SATEM	2014	Generation of false key in the network cannot guarantee file transaction.

IV. CONCLUSION

Various schemes and techniques on MANET security have been discussed and analyzed for their advantages and drawbacks in this paper.

REFERENCES

[1]Immune Inspired Approach for Securing Wireless Ad hoc Networks, *IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.7, July 2009*

[2]Abhijit Das Soumya Sankar Basu Atal Chaudhuri A Novel Security Scheme for Wireless Adhoc Network*, 978-1-4577-0787-2/11 IEEE 2011.*

[3] Prasad Patil Vidyalankar ,Rinku Shah ,Kajal, Enhanced Novel Security Scheme for Wireless Adhoc Networks: ENSS *International Conference & Workshop on Recent Trends in Technology, (TCET) 2012*

[4] Sima Shayog Sharma Viney Dhawan Mandeep Kaur ,Secured Scheme for Ad hoc Networks using Encryption as a Tool, *International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-2, Issue-5),* May 2013**.**

[5] Muthumanickam Gunasekaran and Kandhasamy Premalatha, SPAWN: A Secure Privacy-Preserving Architecture In Wireless Mobile Ad Hoc Networks, *EURASIP Journal on Wireless Communications and Networking 2013.*

[6] Gaurav, Naresh Sharma and Himanshu Tyagi,An Approach: False Node Detection Algorithm in Cluster Based MANET *International Journal of Advanced Research in Computer Science and Software Engineering. Volume 4, Issue 2, February 2014 ISSN: 2277 128X*

[7]T.Manikandan, S.Shitharth, C.Senthilkumar, C.Sebastinalbina, N.Kamaraj , Removal of Selective Black Hole Attack in MANET by AODV Protocol , *International Journal of Innovative Research in Science, Engineering and Technology,March 2014*

[8]S.P.Ramya, Malik, K.Nivetha, V.R.Sindhuja, Secure Communication in Mobile Ad-Hoc Network Using SATEM *Systems*,Nov,2014

[9]W. Stallings, "Cryptography and network security 4th Edition", prentice hall, 2005, PP.58-309.