ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

Anonymous Routing and Secure Transmission in MANET (ARSTNET): Survey

Aleesha Vijayan[1], Yamini.C[2]

PG Scholar, Department of CSE, Dr. N G P institute of Technology, Coimbatore, India[1]

Assistant Professor, Department of CSE, Dr. N G P institute of Technology, Coimbatore, India[2]

ABSTRACT: MANET is an infrastructureless network consists of mobile nodes and the nodes can join and leave the network dynamically. Every movable device can act as router as well as end user. In MANET security is the major concern for the protected communication. Any user can accessible in the MANET, it doesn't depend whether they are legitimate network user or malicious attackers. Anonymity is needed, so that almost all the attacks are avoided. Providing anonymity to the routes, source and destination is a value added technique. Self organizing capability is the major profit and detriment of the MANET. In this paper discussed about security concern of MANET and includes one of the most efficient encryption schemes.

Keywords: Mobile ad hoc networks, Anonymity, Security, Elliptic curve cryptography

I. INTRODUCTION

The novel technology developments in wireless network such as Bluetooth introduce MANET. The growth of mobile phones in MANETs a popular research topic since the mid-1990s. It has self organizing capabilities, so that mobile nodes can join and leave the network dynamically. Each node in MANET moves independent of its location because of that the topology of the group changes dynamically. We need to provide security to the data packets transmitted between the nodes through the respected routes. It is a plane network, the main two features of MANET is node mobility and dynamic topology. These two main features are the reason for the attacks. Malicious user may try to attack the data packets by tracing the route. The malicious attackers may try to find the source and destination through different attacks. The applications of MANET are in military battle field, sensor networks, commercial sectors, medical sectors.

At present MANET do not have any perfect security policy. But it is important to provide secure communication between parties in the MANET, the secure solution which should be dynamic too. So it is necessary to provide anonymity. In some situation anonymity is provided to source and destination. [4]In case of source "notify and go" manner is used. For the destination secrecy, "local broadcasting" is used. [4]In previous papers hop-by-hop encryption and redundant traffic is deployed for packet security. There are different kinds of algorithms and protocols for providing anonymity. The purpose of providing anonymity is by this way we can avoid most of the attacks in the MANET. In the following section discussed about the security attacks, secure routing protocols and also described about the methods of providing anonymity. Due to dynamic topology, distributed operation and limited bandwidth MANET is more vulnerable to many attacks.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

Figure 1: Mobile ad-hoc network.

II. BASICS OF SECURITY ATTACKS

The main two classifications of attacks in MANET are active attacks and passive attacks. These attacks are launched at the different layers of the protocol stack. Passive attacks are a continuous monitoring of the network, there is no direct damage to the network or the data. The information eavesdropped by passive attacker will used for future harmful attacks. These attackers will listen to the communication between the active nodes in the network. The active attacks cause unauthorized state changes in the MANET. In this case the attacker can stop all or parts of the data sent by the communicating parties and modify the content. The active attacks are of two kinds: internal attacks and external attacks. The internal attacks are more severe, because these attacks are caused by actively participated nodes in the network. The following diagram gives the idea about attacks on MANET:

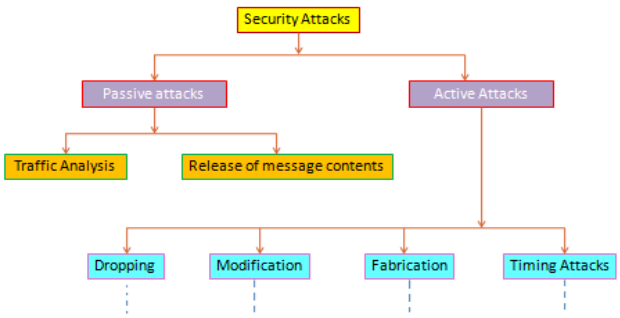

Figure 3: Security Attacks.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

III. LITERATURE REVIEW

[1]In this paper discussed about ECC is utilized for the security enhancement in communication network.ECC is the most efficient public key encryption scheme. Here discussed about the elliptic curve equations for method of key generation instead of conventional equations. The working of ECC is similar to RSA, Diffie-Hellman and Digital signature. The main purpose is for secure communication over the network. It consists of 164 bit key for the secure transfer of the data packet. This scheme provides with low computing power and battery resource usage. The security provided by this scheme depends on the value of the key 'k' and also the parameters should be chosen carefully to avoid attacks in the elliptic curve discrete logarithmic problem. Elliptic curve mathematically is a curve that also forms a group. Here a method is used to produce new points from a known set of points, this method is known as diophantus. This is for improving the speed and accuracy of the operations in the network. In this cryptographic system each user has a private key and public key, so that is Elliptic curve Diffie-Hellman key exchange and elliptical curve digital signature algorithms are the extensions. The main feature of this scheme is greater efficiency in terms of computational overheads key sizes and bandwidth. The performance parameters for elliptic curve cryptography implementation are: higher strength per bit, smaller certificates, storage efficiency. This cryptographic technique guarantees security of smart cards, WSN, WMN.

[2]In this paper a secure distributed cluster formation protocol is used to organize sensor networks into mutually disjoint cliques. The proposed properties of the protocol are here normal nodes are grouped into cliques and all those nodes have same clique membership, So that this cliques exclude outside attackers during the cluster formation. At the same time inside attackers are there, that are detected and take away from the network. This protocol is fully distributed and there is moderate communication overhead. For this ad-hoc network each cluster has cluster head for coordination of the services. For that it uses two types of protocol, that are cluster formation protocol and leader election protocol. The cluster formation protocol is further divided into two categories Leader first (LF) and Cluster First (CF). This paper proposes cluster first approach, that is all the sensor nodes first form clusters, and each cluster then elects its cluster-head. In this approach, exchange information with 1-hop neighbours.

A. PROTOCOL SPECIFICATION:

- Compute its local maximum clique.
- Ordering and updating maximum clique.
- Obtaining final clique
- Check clique agreement
- Spot insider or enforcing clique pact.
- Message authentication is used for finding external attackers.

One problem issued is the node may verify more messages than it signs, so that they propose to choose public key cryptosystem with fast encryption/decryption speed. This happens in fraction of seconds. In case of hostile environment difficult to resist attacks, more over there is no centralized authority.

[3]This paper presents the PRISM protocol which supports anonymous on-demand routing in suspicious location-based MANETs. It relies on group signatures to authenticate nodes, ensure integrity of routing messages while preventing node tracking. It works among any group signature method and any locality-based forwarding mechanism. They evaluate its routing overhead and show that it can outperform anonymous link state based approaches under certain traffic patterns. They also evaluate PRISM's tracking-resistance by comparing its degree of topology exposure to link-state based approaches. PRISM reveals less of the topology and is therefore extra privacy-friendly. This provides privacy against insider and outsider adversaries. Source authenticates the destination and destination authenticates source node. It imports one time secrete key for authentication and encryption. Packets are transmitted based on location forwarding mechanism.

[5]The problem found in this paper is, establishing a shared session key in an authenticated way is addressed. The proposed key agreement protocol assist explicit authentication. The operation explained in this paper, there is a trusted third party such as firewall, to verify the identities of the parties involved in the key agreement session. The benefit is to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

reduce the computational burden at the end user side. In ad-hoc networks asymmetric -key encryption algorithms are used as the solutions, so cryptographic protocols applying over trustless networks.

[6]This paper presents privacy protection in the network, by proposing a secure re-active routing protocol. The main focus of this protocol is to avoid DOS attacks. By this only sender and receiver can have the information that cannot be recognized by other nodes i.e. ., anonymity protection. This protocol has two phases, key establishment and route discovery. During key establishment it generate one secrete key. This protocol consist of three types of routing control packets, that are routing request packet, routing reply packet and routing error packet. For MANET ID based cryptosystem and group signatures are proposed by ISRR routing protocol. When it find DOS attacker the node is removed from the network.

[7]This paper proposed for security and quick communication of data in MANET. It uses attribute based encryption, for that it need details about the next hop. Group signature scheme is used here, so that the member of the group can secretly sign the data. Next is Identity based encryption, is a public key encryption. The attribute encryption is inherited from the identity based encryption. In this a private key associated with attribute set, by using this private key data is decrypted at the receiver side. It Uses BATMAN routing scheme, by this scheme data packets and control packets are randomly generated. For that AUST implements two methods, secrete key generation and proactive routing. This method ensures the confidentiality of the data.

[8]Wireless networks effectively works within the limitation and memory. This paper has been suggested a public key encryption technique for sensor networks within the limited power. This technique ensures confidentiality and authentication. For that play fair cipher matrix and RSA public key encryption technique used correspondingly. The play fair cipher matrix is a symmetric encryption technique; here a pair of letters is encrypted instead of the encryption of the single word. For authentication RSA public key encryption technique with ASCII conversion is used. The RSA algorithm works through the following steps that are key generation, encryption and decryption. The RSA algorithm converts the plain text to cipher text for that ASCII conversion is implemented. First the plain text is converted to ASCII value then encrypt using RSA algorithm after that decrypt the encrypted message and recover the message by ASCII conversion.

[13]In this paper a secure efficient ad hoc distance vector routing protocol is proposed. That is based on the destination –sequenced distance vector routing protocol. This is for bearing the use with nodes of limited CPU processing capability. This protocol guard against DOS attack. Here they proposed to use efficient one-way hash function and do not use asymmetric cryptographic working. This is for supporting the use with nodes of limited CPU power. The detriment of this scheme is that the attackers may create incorrect routing condition.

B. MANET PROTOCOL: DESIGN APPROACHES AND FACTS.

A collection of protocol is used in MANET from the origin for the security of the data transmission. This paper explains about the goals for the secure communication. The security services are provided by the security solutions, that is actually the ultimate goal.

- Availability: Protection from DOS attacks.
- Confidentiality: Should be providing privacy to the data transfer.
- Integrity: Message transmitted over the network never be damaged.
- Authentication: Identification of the nodes and ensure identity of the peer node it is communicate with.
- Non-repudiation: An extension to the identification and authentication service, ensure that the origin of a message cannot deny having sent the message.
- Non-impersonation: No other person can simulate to be new authorized member to learn any useful information.
- Attacks using fabrication: Very difficult to detect and is a false message.

[10] This paper discussed about the IDS and leader election methods. The Intrusion Detection System applied in the MANET , for that it is necessary to select the leader of the cluster among number of nodes, these nodes are battery powered nodes, so that the nodes with stayed energy leaded is elected. The selfish nodes are not appointed for the leader election process. Selfish behaviour in the sense they are saving their own power, and not support other nodes in

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

the cluster. The selected cluster head serves the IDS for that whole cluster. This paper proposes an algorithm for electing the leader, that algorithm uses three messages: election, ACK and leader for fixing the identity of the leader.

The design approaches of MANET protocol described below,

TABLE I
Classification of Protocols

Table-driven(pro-active routing) approach		**On-demand(reactive routing) approach**	
DBF	• Known as Distance Vector Routing Algorithm. • Shortest path routing algorithm.	***AODV***	• Loop free, and avoiding the Bellman Ford "Counting to infinity" problem.
WRP	• Enhanced version of the distance-vector routing protocol. • Maintains an up-to-date view of the network.	***DSR***	• Used in multi-hop wireless ad hoc networks. • It does not use any periodic routing advertisement.
DSDV	• Based on classical Bellman-Ford Routing Algorithm. • To solve the routing loop problem.	***DDR***	• It established network connection to a remote site is only when needed.
OLSRP	• IP routing protocol. • Uses hello and topology control (TC) messages.	***TORA***	• For routing data across Wireless Mesh Networks or Mobile ad hoc networks.

[9]The anonymity provided mainly to source, destination and route. This anonymity provided to the network helps to maintain privacy and integrity. The unfavorable access is avoided by end to end encryption.

C. CLASSIFICATION OF EXISTING ANONYMOUS COMMUNICATION SYSTEM:

- Crypto-system based scheme.
- Routing based scene.
- Broadcasting based scheme.
- Peer-to-peer communication scheme.

One aspect is explained in this paper is pseudonomity, that use pseudonym instead of real name. The author's classify the intrusion detection based on the audit data as hosted based and network based. Before electing the node it is necessary to identify and avoid the selfish nodes. One technique proposed is credit based technique. In this scheme certain payment for nodes is provided to faithfully perform the functions in the network. Another is watch dog is for detection and prevention of the selfish nodes [11] [6].Watch dog is based on passive acknowledgement of the packets by other nodes, through overhearing the transmission. With the proposed work the resource consumption is reduces and also detect the intruders.

[9]In this paper two routing based scheme is discussed, Tor and Crowds. Tor (the second generation onion router) relies on public key cryptography; here encrypt the layer of onion that means the intended receiver only can decrypt the data using private key. Here the next hop has only the information about previous hop. Crowds is similar to the Tor, by

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

this it is difficult to find the identity of the sender. By hiding the IP address, the anonymous network provides security to the user state.

IV CONCLUSION AND FUTURE WORK

In this paper we try to assort the security attacks in MANET. Based on the characteristics of the attacks and by considering the features of the MANET certain techniques are developed for overcoming those attacks. These attacks found in MANETs due to the self organization property and mobility nature. First we briefly discussed about the cryptographic technique used in the wireless network for providing security. We discussed about anonymity concepts in MANET, in fact it is a different method of security solutions. Distinct cryptographic and key managements are comes with anonymity. Then we talk about the cluster formation and cluster head selection, which is for improving the power energy conservation.

Finally, through the survey we also discover several points that may be the future purview of this research paper. Such as cryptographic technique with anonymity protection can get further improved and also it can deals with other techniques related to security.

REFERENCES

[1] Sonali Nimbhorkar, Dr.L.G.Malik , "Prospective Utilization of Elliptic Curve Cryptography for Security Enhancement," International Journal of Application or Innovation in Engineering & Management , Vol.2, Issue.1, pp.87-92, Jan 2013.

[2] Kun Sun, Pai Peng, Peng Ning " Secure Distributed Cluster Formation in Wireless Sensor Networks," 22nd Annual Computer Security Applications Conference, 2006.

[3] Karim El Defrawy, Gene Tsudik, " Privacy-Preserving Location-Based On-Demand Routing in MANETs," IEEE journal on selected areas in communications, VOL. 29, NO. 10, pp.1-10, Dec 2011.

[4] Haiying Shen, Lianyu Zhao," ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs," IEEE Transactions on Mobile Computing, VOL. 12, NO. 6, pp.1079-1093, June 2013.

[5] Mohamed Nabil, Yasmine Abouelseoud, Galal Elkobrosy,Amr Abdelrazek, " New Authenticated Key Agreement Protocols," Proceedings of the International MultiConference of Engineers and Computer Scientists, Vol I, March 2013.

[6] Arun Kumar S, A. Mary Mekala," Effective Anonymous Imperceptible Secure re-active Routing (ISRR) Protocol for MANET," International Journal of Engineering and Technology, Vol 5, No 3, pp.2691-2695, Jun-Jul 2013.

[7] Balaji. S, Manicka Prabha. M,"AUST: Anonymous Unswerving and Secure Transmission in MANET," International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, Issue 3, pp.60-64, March 2013.

[8] Mr.Nisarga Chand, Mr.Bappadittya Roy, Mr.KrishanuKundu, " Designing of an Encryption Technique Suitable For Wireless Ad-Hoc Sensor Network," International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue.3, pp.632-637, March 2013.

[9] Maheshkumar S.Kamble, Hatkar S.S," Anonymous Communication in Computer Networks: A Survey," International Journal of Advanced Research in Computer Science and Software Engineering, , Volume 3, Issue.3, pp.660-664, March 2013.

[10] Kalaivani.R,RamyaDorai.D," Secure Protocol for Leader Election and Intrusion Detection in MANET," International Journal of Advanced Research in Computer Science and Software Engineering,Vol.3, Issue 3, pp.62-66, March 2013.

[11] Alberto Rodriguez-Mayol, Javier Gozalvez, " Improving Selfishness Detection in Reputation Protocols for Cooperative Mobile Ad-hoc Networks," Proceedings of the European Wireless Conference, 2010.

[12] S. Marti, T. J. Giuli, K. Lai, M. Baker, "Mitigating routing misbehavior in mobile ad-hoc networks," Proceedings of the Sixth Annual ACM/IEEE International Conference on Mobile Computing And Networking, pp 255-265, Aug. 2000.

[13] Yih-Chun Hu, David B. Johnson, Adrian Perrig, " SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks,"Journal: Ad Hoc Networks , vol. 1, no. 1, pp. 175-192, 2003.

[14] Supriya Tayal, Vinti Gupta," A Survey of Attacks on Manet Routing Protocols," International Journal of Innovative Research in Science, Engineering and Technology, Vol. 2, Issue 6, pp. 2280-2285, June 2013.

[15] Neha Kaushik, Ajay Dureja," A Comparative Study of Black Hole Attack in MANET," International Journal of Electronics and Communication Engineering & Technology, Vol. 4, Issue 2, pp. 93-102, March – April 2013.

[16] Gagandeep, Aashima, Pawan Kumar," Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review," International Journal of Engineering and Advanced Technology, Vol.1, Issue 5, pp. 269-275, June 2012.

[17] Aarti, Dr. S. S. Tyagi, " Study of MANET: Characteristics, Challenges, Application and Security Attacks," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, pp.252-257, May 2013.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

BIOGRAPHY

Ms.Aleesha Vijayan

She is currently doing her PG in Dr.N G P Institute of Technology, Coimbatore.She Completed her B.Tech in Information Technology from Viswajyothi College of Engineering and Technology, Mahatma Gandhi University, Kerala in 2012. She has attended many of the national level workshops and International conferences. Her areas of interest are Network Security, Wireless Sensor Networks, Mobile Computing, Image processing, Programming etc.

Mrs.C.Yamini

She is currently working as Assistant Professor, dept of CSE in Dr.N G P Institute of Technology, Coimbatore. She completed her B.E in Computer Science and Engineering from Park College of Technology, Coimbatore in 2003. She did her M.E. in Software Engineering from Karpagam University, Coimbatore in 2011. She has 8 years of teaching experience. Fields of Specialization are Programming, Software Testing.