An Optimal key Management for MANET

S.Rajarajeswari
ME Software Engineering
Rajalakshmi Engineering College,,Chennai, TamilNadu, India

S.Baghavathi Priya
Department of InformationTechnology,
Rajalakshmi Engineering College,,Chennai, TamilNadu, India

Abstract- Mobile ad hoc networks (MANETs) can be defined as a collection of large number of mobile nodes that form temporary network without aid of any existing network infrastructure or central access point. Due to the nature of MANETs to design and maintaining security is challenging task for researcher in an open and distributed communication environment. This paper we proposed security architecture for MANET grid and optimal key management by combines symmetric key technique and elliptic curve public key technique. The proposed architecture and optimal key management eliminates threats including the man-in-the-middle attack and the Black hole attack can be effectively eliminated under the proposed scheme. The core advantages of the proposed scheme include strong security, scalability, fault-tolerance, accessibility, and efficiency.

Keywords : Security, Grid, key management, Mobile ad hoc networks (MANETs), attack.

I. INTRODUCTION

WIRELESS cellular system has been in use since 1980s. Wireless system operates with the aid of a centralized supporting structure such as an access point. These access points assist the wireless users to keep connected with the wireless system, when they roam from one place to other. In wireless system the device communicate via radio channel to share resource and information between devices. Due to presence of a fixed supporting structure, limits the adaptability wireless system is required easy and quick deployment of wireless network. Recent advancement of wireless technologies like Bluetooth [3], IEEE 802.11 [4] introduced a new type of wireless system known as Mobile ad-hoc network (MANETs) [1, 2, 5, 6], which operate in the absence of central access point. It provides high mobility and device portability's that enable to node connect network and communicate to each other. It allows the devices to maintain connections to the network as well as easily adding and removing devices in the network. User has great flexibility to design such a network at cheapest cost and minimum time.

MANETs has shown distinct characteristics, such as

- Weaker in Security
- Device size limitation
- Battery life
- Dynamic topology
- Bandwidth and slower data transfer rate

Another characteristic of a MANET is its resource constraints, that is, limited bandwidth and limited battery power. This characteristic makes routing in a MANET an even more challenging task. Therefore, early work in MANET research focused on providing routing service with minimum cost in terms of bandwidth and battery power.

Currently, several efficient routing protocols have been proposed. These protocols can be classified into two categories: reactive routing protocols and proactive routing protocols. In reactive routing protocols, such as the Ad hoc On Demand Distance Vector (AODV) protocol nodes find routes only when required. In proactive routing protocols such as the Optimized Link State Routing (OLSR) protocol nodes obtain routes by periodic exchange of topology information.

Most of these routing protocols rely on cooperation between nodes due to the lack of a centralized administration and assume that all nodes are trustworthy and well-behaved. However, in a hostile environment, a malicious node can launch routing attacks to disrupt routing operations

II. MANET APPLICATION

With the increase of portable devices as well as progress in Wireless communication, ad hoc networking is gaining Importance with the increasing number of widespread Applications. Ad hoc networking can be applied anywhere where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. The set of applications for MANETs is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infrastructure environment into the ad hoc context a great deal of new services can and will be generated for the new environment. It includes

- Military Battlefield
- Sensor Networks
- Commercial Sector
- Medical Service
- Personal Area Network

III. SECURITY PROBLEM WITH EXISTING MANET

The main theme of the previously presented ad hoc routing protocols and communication system is that all anticipating nodes work fine with good faith and without maliciously disrupting the operation[7,8,9] such as vulnerable to denial of service attacks [10], and security holes may exist which permit hacking into the smart meters to manipulate usage data. However, the existence of malicious entities cannot be disregarded in any system, especially in open ones like ad hoc networks. In ad hoc network the routing function can be disrupted by internal or external attackers. The attacker can be any legitimate participant of the routing protocol. An external attacker is defined as any other entity. Cryptographic solutions can be employed to prevent the impact of external attackers by mutual authentication of the participating nodes through digital signature schemes [11]. However, the underlying protocols should also be considered since an attacker could manipulate a lower level protocol to interrupt a security mechanism in a higher level. Internal attackers having capability to complete access the communication link they are able to advertise false routing information at will and force arbitrary routing decisions on their peers.

A. Security Goals

- Authentication
- Confidentially
- Integrity
- Availability
- Non-repudiation
- Access Control

Some of security threads which are challenging in MANET design are.

3.1. Denial of service

Denial of Service (DoS) is any event that diminishes or eliminates a network's capacity to perform its expected function [16]. One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately

3.2. Man-in-middle-attack

A man-in-the-middle attack can succeed only when the attacker can impersonate each endpoint to the satisfaction of the other. It is an attack on mutual authentication . Most cryptographic Protocols include some form of Endpoint authentication specifically to prevent MIM attacks

3.3. Black hole

In a blackhole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm and lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the centre. Because nodes on, or near, the path that packets follow have many opportunities to tamper with application data, sinkhole attacks can enable many other attack

3.4 Reply

In a MANET, topology frequently changes due to node mobility. This means that current network topology might not exist in the future. In a replay attack, a node records another node's valid control messages and resends them later. This causes other nodes to record their routing table with stale routes. Replay attack can be misused to impersonate a specific node or simply to disturb the routing operation in a MANET.

IV. OVERALL ARCHITECTURE FOR MANET GRID

Let us consider a scenario that we gather a group of Adhoc nodes to form a grid. From the grid we select a node as a node which can able to communicate with all other nodes. And we assume that node as trusted node knows as trusted anchor. Any request any nodes with in grid will forward the request to trusted Anchor. The followings are the corpus requirements for a typical MANET Grid as follows

- Group Signature Generator
- Trusted Anchor
- Hybrid key (Symmetric and elliptical cure key) Generator
- Session key Generator
- Collector and session key manager

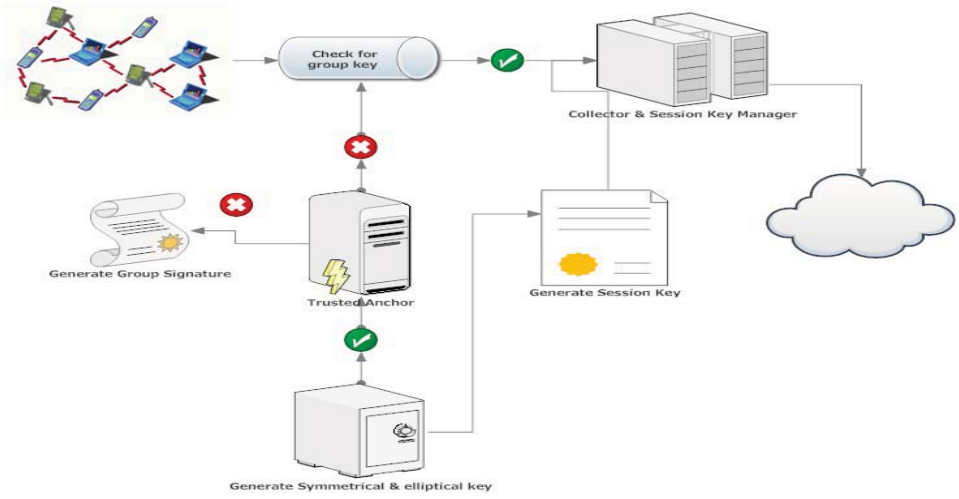

Figure 1 A typical MANET Grid

4.1 Group Signature Generator

Group key Generator module ensure for group key signature if any node have the group key it forward the request to symmetric and elliptic key generator. If any node does not have the group, it checks for valid information (state

information check for history).If the information is trustable it generates a symmetric group key and sent it to the requester. To generate Group signature we use AES algorithm.

4.1.1 AES Algorithm

The block to be encrypted is just a sequence of 128 bits. AES works with byte quantities so we first convert the 128 bits into 16 bytes. We say "convert," but, in reality, it is almost certainly stored this way already. Operations in RSN/AES are performed on a two-dimensional byte array of four rows and four columns. At the start of the encryption, the 16 bytes of data, numbered D0 -D15, are loaded into the array. Each round of the encryption process requires a series of steps to alter the state array. The input to the encryption and decryption algorithm is a single 128-bit block, is depicted as a square matrix of bytes. This block is copied into the State array, which is modified at each stage of encryption or decryption. After the final stage, State is copied to an output matrix. The final round of both encryption and decryption consists of only 3 stages

4.2 Hybrid key Generator

The hybrid key generator generates an elliptic key. It also generates a symmetric key which encapsulate elliptic key and forward it to session key generator to generate a session key to regulate the communication. For hybrid key generation two algorithms are used Blow fish algorithm And ECC.

The following are the functionally of Symmetric and elliptical cure key management module

1. Generate Symmetric key
2. Generate elliptical curve key.
3. Store the hybrid key in key store

4.2.1 Blowfish Algorithm

Blowfish is a variable-length, a new secret-key block cipher. It is a Fiestal network, iterating a simple encryption function 16 times. Variable-length key, 64-bit block cipher. The algorithm consists of two parts: a key-expansion part and a data- encryption part. Key expansion converts a variable-length key of at most 56 bytes (448 bits) into several sub key arrays totaling 4168 bytes. Data encryption occurs via a 16-round Feistel network. Each round consists of a key-dependent permutation, and a key- and data-dependent substitution. The additional operations are four indexed array data lookups per round. Implementations of Blowfish that require the fastest speeds should unroll the loop and ensure that all sub keys are stored in cache.

The sub keys are calculated using the Blowfish algorithm. The exact method is as follows:

1. Initialize first the P-array and then the four S-boxes, in order, with a fixed string. This string consists of the hexadecimal digits of pi (less the initial 3).

2. XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to P14). Repeatedly cycle through the key bits until the entire P-array has been XORed with key bits.

3. Encrypt the all-zero string with the Blowfish algorithm, using the sub keys described in steps (1) and (2).

4. Replace P1 and P2 with the output of step (3).

5. Encrypt the output of step (3) using the Blowfish algorithm with the modified sub keys.

6. Replace P3 and P4 with the output of step (5).

7. Continue the process, replacing all entries of the P- array, and then all four S-boxes, with the output of the continuously-changing Blowfish algorithm

4.2.2 Elliptic Curve Cryptography

Public-key cryptography is based on the intractability of certain mathematical problems. Early public-key systems are secure assuming that it is difficult to factor a large integer composed of two or more large prime factors. For elliptic-curve-based protocols, it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is infeasible. The size of the elliptic curve determines the difficulty of the problem. The primary benefit promised by ECC is a smaller key size, reducing storage and transmission

requirements—i.e., that an elliptic curve group could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key . Elliptic curve cryptography is a public key cryptosystem that relies on the believed difficulty of the elliptic curve discrete logarithm for its security .An elliptic curve group could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key a 256-bit ECC public key should provide comparable security to a 3072-bit RSA public key The elliptic curve is defined by the constants a and b used in its defining equation. Finally, the cyclic subgroup is defined by its generator G. For cryptographic application the order of G, that is the smallest non-negative number n such that, nG= ∞ is normally prime. Since n is the size of a subgroup of E (Fp) it follows from Lagrange's theorem that the number $h = \frac{|E(F_p)|}{n}$ is an integer. In cryptographic applications this number h, called the cofactor, must be small (h≤4) and, preferably, h=1.

4.3 Session key Generator

The trusted anchor forwards the request to session key generator if the request contains a valid group key signature the session key generator generates a session key and forwards the session key to collector and to the requester to maintain a session between source and destination. If the transaction get completed or time expired session key generator will disable the session key. Session key will be generated using Rijndael Algorithm. Rijndael also defines a method to generate a series of sub keys from the original key. The generated sub keys are used as input with the round function. As input, Rijndael accepts one-dimensional 8-bit byte arrays that create data blocks

The following are the functionality of Session manager module

1. Generate session key and store it in key store
2. Disable session key.

4.3.1 Rijndael Algorithm

Rijndael is the block cipher algorithm recently chosen by the National Institute of Science and Technology (NIST) as the Advanced Encryption Standard (AES). It super cedes the Data Encryption Standard (DES). Rijndael is an iterated block cipher. Therefore, the encryption or decryption of a block of data is accomplished by the iteration (a round) of a specific transformation (a round function). . Rijndael also defines a method to generate a series of sub keys from the original key. The generated sub keys are used as input with the round function. As input, Rijndael accepts one-dimensional 8-bit byte arrays that create data blocks. The plaintext is input and then mapped onto state bytes. The cipher key is also a one-dimensional 8-bit byte array. To encipher a block of data in Rijndael it performs an Add Round Key step (XORing a sub key with the block) by itself, then the regular transformation rounds, and then a final round with the Mix Column step omitted. The cipher itself is defined by the following steps

An initial Round Key addition

- Nr-1 Rounds;
- A final round.

The round transformation is broken into layers. These layers are the linear mixing layer, which provides high diffusion over multiple rounds. The non-linear layer which are basically applications of the Rijndael S-box. And the key addition layer which is simply an exclusive or of the round key and the intermediate state. Each layer is designed to have its own well-defined function which increases resistance to linear and differential cryptanalysis

4.4. Collector and session key manager

The session key manager initially checks for session key , if session key found ,the validity of the session key will be checked .For a valid session key the source node request will accepted and a communication will be establish through the collector to the corresponding destination. The process will be repeated for each transaction. In case if the session key is not a valid one then the request is forwarded request is denied.

1. Maintain record of session key
2. Maintain session between the communications
3. Provide a connection to corresponding destination node

4.4.1 Needham–Schroeder protocol

Needham–Schroeder protocol can refer to one of the two communication protocols intended for use over an insecure network, both proposed by Roger Needham and Schroeder. Since in the Needham-Schroeder authentication protocol [13], the only-once semantics on involved messages is crucial to countermeasure the replay attacks [12], message times-tamping or the use of nonce is normally considered sufficient against replay attack [14]. The Needham–Schroeder Symmetric Key Protocol is based on a symmetric encryption algorithm. It forms the basis for the Kerberos protocol. This protocol aims to establish a session between two parties on a network, typically to protect further communication. The Needham–Schroeder Public-Key Protocol, based on public-key cryptography. This protocol is intended to provide mutual authentication between two parties communicating on a network, but in its proposed form is insecure

V. SECURITY MECHANISM FOR OF PROPOSED MANET GRID

In this section, we propose an authentication scheme, which applies an elliptic curve public key cryptography to the Needham-Schroeder protocol. Via a trust anchor, the public key method is employed to establish symmetric keys for agents to communicate with each other.The proposed security mechanism is very effective and robust. The group key eliminated malicious nodes by checking the routing information and valid group key so malicious attack and Sybil attack can be prevented. Whenever a node wish to communicate it should be registered by getting the group key so unauthorized node cannot participate in the communication which eliminate men-in-middle attack. The Session key manager maintains a session between nodes so that the black hole attack can be eliminated. The proposed Architecture efficiently eliminates most of the attacks. Hence the proposed theme is powerful and robust in security credentials

VI. CONCLUSION

An optimal key management mechanism is proposed to ensure the security credentials across the nodes. The proposed security mechanism implements public key infrastructure and the secure Needham-Schroeder authentication protocol. It has shown that the known threats including the man-in-the-middle attack and the replay attack can be effectively eliminated under the proposed scheme. The proposed mechanism can prevent most of attach by maintaining session between the communication parties. The optimal key management scheme provides strong security, scalability, fault-tolerance, accessibility, and efficiency.

VII. ACKNOWLEDGMENTS

I wish to thank Dr.S.Poonkuzhali, Professor and Head of the Department ,Department of Information Technology , Rajalakshmi Engineering college for extending all facilities to me to work on this paper. I would like to express my sincere appreciation and gratitude to my guide Mrs.S.Baghavathi priya, Associate Professor, Department of Information Technology, Rajalakshmi Engineering College, for her guidance , constant encouragement and support. Her meticulous attention and creative thinking has been a source of inspiration for me throughout this paper.

REFERENCES

[1] B. Dahill, B. N. Levine, E. Royer, and C. Shields, "A secure routing protocol for ad hoc networks," in Proceedings of the International Conference on Network Protocols (ICNP), pp. 78-87, 2002.
[2] Y. Hu, A. Perrig and D. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, in Proceedings of ACM MOBICOM'02, 2010.
[3] Janne Lundberg, Routing Security in Ad Hoc Networks. Tik-110.501 Seminar on Network Security
[4] http://citeseer.nj.nec.com/400961.html.2000.H. Dang, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks", IEEE Communications Magazine, 0163-6804, pp. 70-75, October 2009.
[5] Jean-Pierre Hubaux, Levente Buttyan, Srdjan Capkun. The Quest for security in Mobile Ad Hoc Networks. Proceedings of the 2010 ACM International Symposium on Mobile ad Hoc networking & computing, Long Beach, CA. 2001.
[6] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks," Security Protocols, 7th International Workshop, LNCS, Springer-Verlag, 2009
[7] Y.C. Hu, D.B. Johnson and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," IEEE, Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02), 0-7695-1647-5, 2010
[8] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," IEEE Security Privacy, vol. 7, pp. 75–77, 2009.
[9] Z. Fan, G. Kalogridis, C. Efthymiou, M. Sooriyabandara, M. Serizawa, and J. McGeehan, "The new frontier of communications research: Smart grid and smart metering," in e-Energy'10: Proc. 1st Int. Conf.Energy-Efficient Compute. Netw., New York, 2010, pp. 115–118.
[10] T. Flick, "Hacking the smart grid," presented at the Black Hat USAConf., Las Vegas, NV, 2009.
[11] "TEMPORALLY-ORDEREDROUTING"http:// en.wikipedia.org/wiki/Temporallyordered_routing_algorithm
[12] S. M. Bellovin and M. Merritt, "Limitations of the Kerberos authentication system," ACM Compute. Commun. Rev., vol.20, no.5, pp.119–132, Oct. 1990.
[13] R. M. Needham and M. D. Schroeder, "Using encryption for authentication in large networks of computers," Common. ACM, vol. 21, no.12, pp. 993–999, Dec. 1978.
[14] D. E. Denning and G. M. Sacco, "Timestamps in key distribution pro-tools," Common. ACM, vol. 24, no. 8, pp. 533–536, Aug. 1981The following are the functionality of trusted anchor