

ENHANCING SECURITY FOR MANETs USING DISCRETE KEY GENERATIONS

H. ATEEQ AHMED¹, K. SAMSON PAUL², B. HARISH KUMAR REDDY³

¹Assistant Professor of CSE, Dr. K.V. Subba Reddy Institute of Technology, Kurnool, Email: ateeqh25@gmail.com.

²Assistant Professor of CSE, Dr. K.V. Subba Reddy Institute of Technology, Kurnool, Email: kakarlasamson1984@gmail.com.

³Assistant Professor of CSE, Dr. K.V. Subba Reddy Institute of Technology, Kurnool, Email: harish8099@gmail.com.

Abstract

Mobile Ad Hoc is a network connection method which is most often associated with wireless devices. The connection is established for the duration of one session and requires no base station. Instead, devices discover others within range to form a network for those computers. These networks often suffer with a problem of Malicious attacks from different types of attackers. Many attacks which often occur are based on the principle of Authentication, Confidentiality & Integrity. MANETs tends to be very prone to complex types of attacks as it is very easy for the attacker to gain control on it due to its inadequate Security mechanism. In this paper, a proposed scheme is narrated which will further strengthens the Mechanism of Security. Instead of using a Unique key, Discrete keys are used for Encryption & Decryption mechanisms.

Key Words: Multi signature, Proxy signature, Advanced threshold cryptography, Discrete Keys.

1. INTRODUCTION

The purpose of these requirements is to protect the exchanged effective security architecture must ensure are explained in the following: Security is essential to keep off hackers, intruders, viruses and industrial espionage.

1.1 Availability

The term Availability means that a node should maintain its ability to provide all the designed services regardless of the security state of it.

1.2 Confidentiality

In other words, in order to maintain the confidentiality of some confidential information, we need to keep them secret from all entities that do not have the privilege to access them.

1.3 Integrity

Integrity ensures the identification of the messages while they're transmitted. Integrity may

be compromised especially in ways: Malicious changing and Accidental changing. A message may be removed, replayed or revised through an adversary with malicious goal, that's seemed as malicious changing; at the contrary, if the message is misplaced or its content material is modified because of a few benign failures, which can be transmission mistakes in conversation or hardware mistakes along with tough disk failure, then it's far classified as unintended changing.

1.4 Authentication

Authenticity is essentially assurance that participants in communication are genuine and not impersonators. It is necessary for the communication participants to prove their

identities as what they have claimed using some techniques so as to ensure the authenticity.

2. AUTHENTICATION USING KEY SHARING

Particularly, in ad hoc networks authentication means to provide validation of the peer identity in an association, using digital signature. A common principle of security engineering is that one should not rely on a single line of defense, so researchers propose the sharing of secrets. In secret sharing, the secret is first shared among the parties who later reconstruct it while in Threshold Cryptography the secret is assumed as a shared input to a cryptographic computation, it is never reconstructed rather computed providing security against forging and exposure of private keys etc. For secure authentication the digital signature is computed in a distributed way based on the shares of secret key, therefore taking idea of secret sharing from Shamir's secret sharing scheme [1] the idea of Threshold signature was developed and applied to MANETs following the procedure in the below given definition.

Thresh-Sig: is the distributed signature protocol. The output of the protocol is a signature Sig on message M.

Ver: is the verification algorithm on input M, Sig, and Pk, checks if Sig is a valid signature of M under Pk.

3. SECURITY ATTACKS IN MANETs

There are two different types of attacks that can happen to a network. They are active attacks and passive attacks. Active attacks are attacks that alter the content of the data. These attacks can degrade the network performance significantly or bring down the network, such as denial of service. These attacks may be the root cause for network traffic, incorrect

service or the complete network may get shattered. The dynamic nature of MANET makes it susceptible to several security breaches. The attacks observed in MANET can be categorized into two types. They are active and passive attacks. Thus, it is mandatory to sniff all such unwanted activities in the bud, such that the system can serve its purpose effectively.

3.1 Passive attacks

A passive attack does not disrupt the operation of the protocol but tries to discover valuable information by listening to traffic. Passive attacks may happen by illegal listening, which is a serious threat to privacy and confidentiality. Illustration of passive attack is given in Figure 3.1.

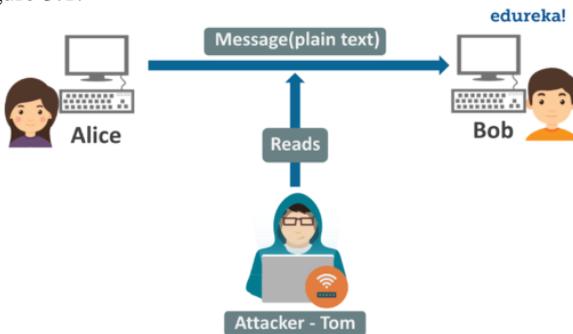


Figure 3.1: Passive Attacks

- a) Black hole: all packets are routed to a specific node which will not forward them at all.
- b) Routing loops: cause a loop in routing path.
- c) Network partition: the network is divided into sub networks where nodes cannot communicate each other even though path exists between them.
- d) Selfishness: A node will not serve as a router for other nodes.
- e) Sleep deprivation: A node is forced to use up its battery.
- f) Denial of Service: A node is prohibited from sending or receiving packets.

3.2 Active attacks

An active attack injects arbitrary packets and tries to disrupt the operation of the protocol in order to limit availability. Active attacks may be carried out through packet tampering, node cloning, packet deletion and replication. Illustration of active attack is given in Figure 3.2.

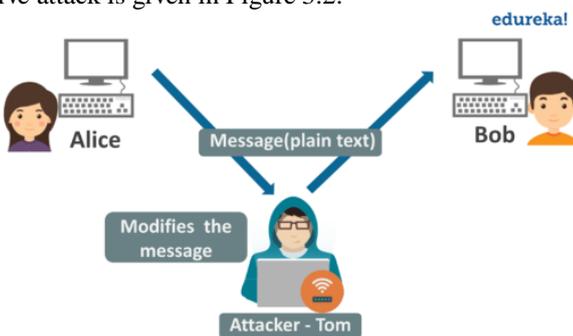
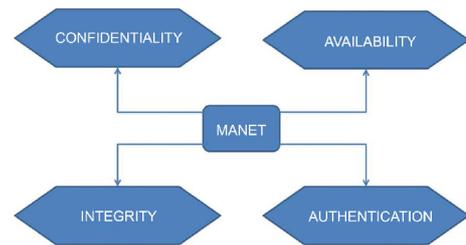


Figure 3.2: Active Attacks

- a) Cache poisoning: information in routing tables is modified, deleted or contains false information.
- b) Packet dropping: A node drops packets that are supposed to be routed.
- c) Spoofing: insert packet or control message with false or altered source address.

4. SECURITY ISSUES

For MANETs, there are several security related issues. The security solution for MANETs is to provide security services such as Confidentiality, Integrity, Availability, and Non-Repudiation. We describe and discuss about these major security issues taking cryptographic techniques under consideration.



Authentication: To identify a node or user in ad hoc network, secure authentication is required. The basic objective is to save honest users from being cheated and to prevent impersonation. Digital signature is the technique which is used for the purpose effectively. A signature is shared among users and regenerated when needed, is the basic idea behind threshold signature schemes. But sometimes a user grants the signing authority to another user as we have observed in proxy signature which is a threat for other users. Another potential threat is, if a group of malicious user attacks collusively such as n users impersonate the other n user's signature could harm the smoothness of system until it shall be resolved. For this purpose CA and ID-based schemes based on threshold cryptographic primitives have been designed. Either CA assigns a key or ID to user which is used to generate the share of signature known as partial signature. Partial signatures and threshold signatures are generated as the function of ID and verified. These partial signatures then are combined to form threshold multi-signatures. New techniques are being developed to reduce the danger of Key escrowing and with reduced computation especially for MANETs.

Confidentiality: Another important security feature is confidentiality which means the contents of secret message should not be disclosed to any other user but the one to whom secret information has been sent. MANETs are open networks and therefore, communication over such networks requires a verifiable identity as remote users may not know each other. This verification process detects the sender which helps to find out that if the message is forged or the signature has been stolen or the authorized user is behaving unkindly. All these problems are considered when security of MANET is concerned. Threshold digital signatures

provide a way to build confidentiality as only a legal user can only open the message.

Non-Repudiation: The major goal achieved by implementing non-repudiation is to ensure that if a user sends a message with the signature then that user cannot deny having sent the message.

Availability: The objective of availability is to keep the network service or resources obtainable to the authorized users. It permits the survivability of the network despite malicious incidents such as DoS (Denial of Service) attack. When a dishonest node launches a DoS attack or tries to disturb the communication between nodes generating some erroneous messages, an intrusion detection process is taken place. In such process a periodically monitoring of the current activities of all participating nodes is done.

Integrity: It shows that received message is not modified or corrupted. When data or secret information is sent through the wireless medium, there is a possibility that an intruder picks up message and resend with incorrect information. Integrity can be achieved through digital signature or hash function algorithms.

5. OUR SOLUTION

There are various methodologies adopted which are given below.

5.1 Solution to One Point Failure & Nodes Authenticity

The use of a single CA (certificate authority) will be the vulnerable point in an Ad-hoc network, therefore the idea of distribution of CA is used that is K out of N nodes are required to take the action. Parameters N and K can be selected in such a way that the number of CA nodes in the network is adequate to provide robust certification services. Therefore gives a distributed self-organized CA, which does not rely on any central or external authority. To make threshold signature scheme more secure against malicious acts, [1] proposed the verifiable IP-address binding with public key. Each square region has a specific number of nodes= N . Author claims that this IP-bound threshold signature scheme not only provides a user simultaneous message authentication but also implicit public-key authenticity. The best authentication scheme is one with threshold cryptography and distributed CA capabilities [2].

The scheme proposed by [2] defines a rectangular topology, as given in figure 1, which assumes uniform distribution of the nodes in the smaller square region. Suppose that the coordinates of two mobile nodes are (x_1, y_1) and (x_2, y_2) respectively. These two nodes will be able to communicate, if the following inequality holds:

5.2 Key Disclosure and Key Management Solution

There are two schemes for key management PKI (Public Key Infrastructure) which is CA-based and another is ID-based introduced by Shamir in 1984. ID-based systems can be a good alternative for CA-based systems from the viewpoint of efficiency and convenience. It uses the identity

of user as public key and computes the private key as the function of public key; moreover user's credibility and trust management can omit the need of a secure channel. CA-based key distribution schemes have some drawbacks such as certificate validity and verification. Proposes id-based scheme for keys management using elliptic curve groups and bilinear maps, scheme works as a KGC register the new user and maintain a data base for necessary details.

User can select any $t+1$ out of n KPAs (Key Privacy Authorities) to obtain all partial keys to compute private key. IBTKIE (Identity-based Threshold Key Insulation Encryption) is another time based key management scheme proposed by [5]. In this scheme for a certain time duration at least k out of n helpers are needed to update the user's temporary private keys. Combining at least k ID key update information shares with one temporary private key corresponding to another period t' , user ID can derive the temporary private key for the current period t . Distributed key when used for jointly such as for conferences can be constructed as mentioned above.

5.3 Solution to proactive multi-secret Sharing Threshold Schemes

For threshold multisecret sharing two schemes are in use CA-based and ID-based as proposed by. CA-based scheme requires a secure channel to issue certificate while identity based needs a lot of computational work. Using the concepts of bilinear pairing, distributed key generation and joint Pedersen verifiable secret sharing scheme [8] proposed the solution related to problems of security in open networks. A proactive secure scheme based on discrete logarithm DKMI (Distributed Key Management Infrastructure) is introduced in [7] that consider secret distribution, updating and redistribution using DKRU that solves the problem of the faulty share holders by identifying them in first round.

5.4 Solution to Proxy Signature Problem

For a valid Proxy signature, two or more proxy signers out of n can cooperatively produce it presents the security analysis of an ID based solution for forgery attack and shows that the scheme has some flaws however after correcting a new solution can be designed gives another solution based on KC-scheme making use of RSA and Lagrange interpolation to generate the proxy signature. A verification is performed for valid proxy signer to make scheme more secure and robust. Another solution is proposed in [6] to overcome the problem for an attack by original signer. The scheme works as the original signer say P_0 chooses shares for each member in the proxy signer group and send them via a secure channel, P_0 then selects time duration and divides it into short periods and generates secret shares with some useful information like public key valid delegation period etc, for these periods. Upon receiving these shares, proxy signers compute individual proxy signature send them back to designated clerk who after verification compute the signature and then a verification is performed using parameter ASID which shows the actual signer id. For the scheme if attackers try to forge or calculate the private information from public

information it's not possible due to provided computation security using discrete logarithm.

Table -1: Key sizes in bits for equivalent levels

SECURITY BITS	SYMMETRIC ENCRYPTION ALGORITHM	MINIMUM SIZE (BITS) OF PUBLIC KEYS		
		RSA	ECC	KEY SIZE RATIO OF RSA VS ECC
80	SKIPJACK	1024	160	6:1
112	3DES	2048	224	9:1
128	AES-128	3072	256	12:1
192	AES-192	7680	384	20:1
256	AES-256	15360	512	30:1

[6] M. S. Hwang , S. F. Tzeng, and C. T. Li."A New Non-repudiable Threshold Proxy Signature with Valid Scheme Delegation Period". Gervasi and M. Gavrilova (Eds.): ICCSA 2007, LNCS vol 4707, Part III, pp. 273-284, Springer, Heidelberg.

[7] M. S. Hwang , S. F. Tzeng, and C. T. Li. "A Fully Distributed Proactively Secure Threshold-Multisignature Scheme". In IEEE Transaction on Parallel and Distributed Systems, VOL. 18, NO. 4, APRIL 2007

[8] W. Chen and F. Lei. "An Efficient Multi-sender Identity Based Threshold Signcryption with Public Verifiability". In Eighth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2007.

6. CONCLUSIONS

With Observation of a range of techniques to authenticate an individual signer or a group of signers, we conclude that Using Discrete Key Structures in providing security to MANETs in term of public key management, partial signature aggregation and entity management structure for dynamically adjustable groups. In spite of complexities in implementation, there are techniques such as weighted RSA technique and use of AES based Threshold cryptography to overcome the problem. Trust building among nodes without a central authority is the future challenge in the field of cryptography.

7. REFERENCES

[1] S. Iftene and M. Grindei. "Weighted Threshold RSA Based on the Chinese Remainder Theorem". In Ninth International Symposium on Symbolic and Numeric Algorithms for Scientific Computing-2008

[2] G. D. Crescenzo, R. Ge and G. R. Arce. "Improved Topology Assumptions for Threshold Cryptography in Mobile Ad Hoc Networks". In ACM SASN, 2005.

[3] D. D. Vergados and G. Stergio. "An Authentication Scheme for Ad-hoc Networks using Threshold Secret Sharing". Wireless Pers Commun (WPC'07) vol 43 ppt. 1767-1780, Springer 2007.

[4] M. A. Azer ,S. M. El-Kassas and M. S. El-Soudani . "Threshold Cryptography and Authentication in Ad Hoc Networks ". In Second International Conference on Systems and Networks Communications (ICSNC'07), 2007.

[5] J. Weng, S. Liu, K. Chen, D. Zheng, and W. Qiu. "Identity-Based Threshold Key-Insulated Encryption without Random Oracles". In T.Malkin (Ed): CT-RSA 2008,LNCS vol 4964 pp. 2013-220. Springer, Heidelberg 2008.