IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 05-10
www.iosrjournals.org

A Review On Secure Key Management In Ad-Hoc Network

[1]Aniket L Joshi
[1]*Department of Computer technology, Rajarshi Shahu College of Engineering, Pune, India.*

Abstract: *An ad hoc network is a decentralized type of network. The network is ad hoc because it does not have a pre-existing infrastructure. An ad hoc network is a common wireless network that can communicate with each other without any centralized administration or pre-existing infrastructure. Due to nature of Inconstant Wireless medium Data Transfer is a major problem in ad hoc it lacks Security and Reliability of Data. Cryptographic techniques are often used for secure Data transmission wireless networks. Most cryptographic technique can be symmetric and asymmetric, depending on the way they use keys. However, all cryptographic techniques is good for nothing if key management is weak. There are various type of key management schemes that have been proposed for ad hoc. In this survey, we present a complete study of various key management techniques to find an efficient key management for Secure and Reliable Data transmission in ad hoc.*

Keywords: *Ad-Hoc network, Security issues, Key Management.*

I. Introduction

An Ad Hoc network is a collection of wireless nodes that communicated with each other without any centralized administration (node). Ad Hoc network is kind to peer-to-peer networks, where there is no fixed infrastructure (i.e. network is formed on demand, and have a fully dynamic network topology. There is no central authority and ad hoc network is self – organizing and adaptive .Node forming in ad hoc network is often low energy, portable small devices. Ad Hoc network may be ideal different from the other network in computer science classrooms an Ad Hoc network could form between students PDA and the workstation of the teacher [1].

II. Security Issues

2.1 Security Goal for Ad-Hoc Network [2]

2.1.1 Confidentiality: Confidentiality ensures that only authorized person can have access to certain information. Classified information application that uses ad hoc network like in military operations, certain information can be appropriate. Therefore, disclosure of such information can be high in price.

2.1.2 Availability: Availability ensures that the requested service should be available as when requested. So availability opposes Denial of Service (DOS). With denial of service attack competitor can also break down important services like key management. Therefore, availability is an important security goal that should be achieved with any kind of ad hoc network application.

2.1.3 Integrity: Integrity implies that message should be unaltered during its transmission from source to destination. Message can be modified Un-intentionally during transmission considering of radio propagation. A malicious attacker can also modify a message intentionally during its transmission.

2.1.4 Authentication: Authentication is the process of identification, that a receiving entity is been assured that message he receives come from an authorized source. In an ad hoc network, mobile node is vulnerable to compromise without proper authentication an attacker can authenticate user and thus can have the full control of the entire network.

2.1.5 Non-Repudiation: Non-Repudiation implies that once message sent, the sender cannot deny that they ever sent or received such a message. It is an important security service by which compromised node can detect and isolated.

2.2 security attack [3]

2.2.1 Passive Attack: In passive attacks, an originator captures the data without altering it. The attacker does not modify the data and does not edit any additional data. The main goal of attacker is to obtain information that is been transmitted.

2.2.2 Active Attack: In Active attacks an attacker actively participates in distort the normal operation of the network services. An attacker can create an active attack by modifying packets or by modifying the information or giving the false information.

Active attack can divided into two major groups:
a) Internal attack: are forms compromised nodes that were once an authorized part of the network. Since the already part of the network as authorized nodes, they are much more secure and difficult to detect as compared to external attack.
b) External attack: These attacks get carried by node that is not an authorized part of the network.

2.3 Key Issues and Challenges [4]

2.3.1 Link Level Security: Nodes in ad hoc network communicate by wireless link, which is much vulnerable to various active and passive attacks. Absence of security mechanism like firewall, access control leads a node in an ad hoc network attacks. Attacks like impersonating a node, traffic re-direction, denial of service etc. Make it hard to achieve the prime security goals.
2.3.2 Secure Routing: Most of the researches in the area an ad hoc networking lead to obtain a secure routing protocol for mobile ad hoc network, which is hard to achieve. In most of the routing protocol in mobile ad hoc networks, intermediate nodes are acting as disseminate. So if a node is compromised, then it can generate false routing protocol information, spread previous routing information, insert new information with existing information, which will finally break down the whole network. Sometime node can act meanly to save own battery power. A compromised node can also send malicious information to other nodes, which in turn attacks other nodes in the network.
2.3.3 Key Management: Key management is one of the prime requirements in any secure network. In ad hoc networks, have no fixed infrastructure, no central authority and connectivity does not always guaranteed, Key management becomes a key issue for securing ad hoc networks. The key management issues have discussed in detail.
2.3.4 Dynamic Mobility: One of the major characteristic of an ad hoc network is the node is dynamic in nature. Nodes can join or leave in ad hoc network at any time and thus there is no guaranteed connectivity between nodes. Static security mechanisms are not always suitable for ad hoc network. Therefore, this property of ad hoc network makes it difficult for the researchers come up with secure key management and routing protocol.

III. Key Management In Ad Hoc Network

Cryptography is a powerful tool in achieving security. Mostly cryptography is been used for secure, Robust and efficient key management subsystem. Key management is a basic main part of security of ad hoc network. Some of symmetric and asymmetric key management scheme has purposed in the ad hoc network. Key management used with Key Generation Key distribution, Key storage, updating keys, Revocation, deleting, arching and using the key acing to secure.

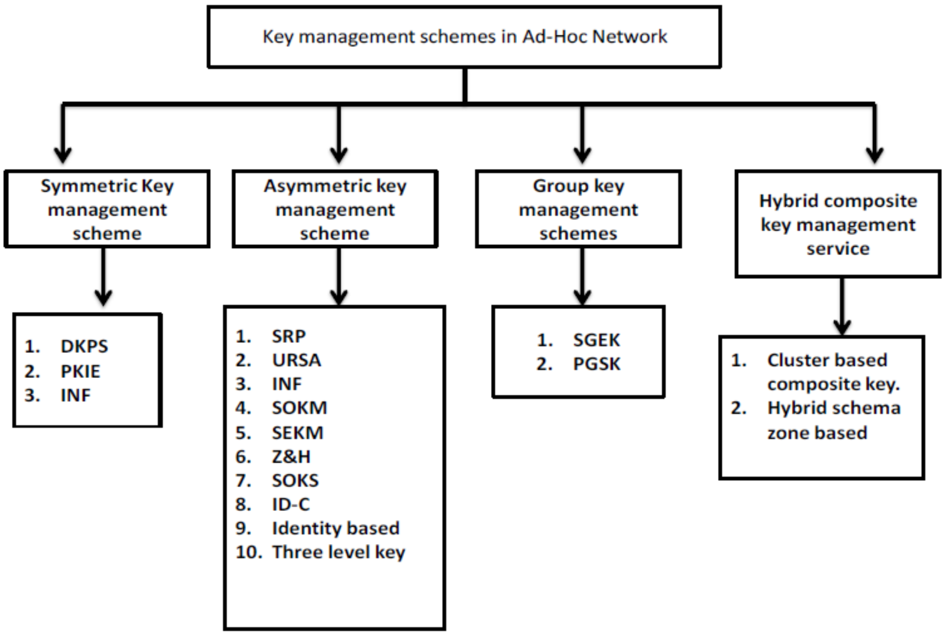

Key management schemes in Ad-Hoc Network
Symmetric Key management scheme
Asymmetric key management scheme
Group key management schemes
Hybrid composite key management service
1. DKPS
2. PKIE
3. INF
1. SRP
2. URSA
3. INF
4. SOKM
5. SEKM
6. Z&H
7. SOKS
8. ID-C
9. Identity based
10. Three level key
1. SGEK
2. PGSK
1. Cluster based composite key.
2. Hybrid schema zone based

Figure2: Key Management Scheme in Ad hoc Network

3.1 Symmetric Key Management in Ad hoc Network

In symmetric key management sender and receiver uses same key. This keys used for encrypting the data as well as for decrypting the data. If n nodes want to communicate in Ad -hoc network number of keys are required, where k = n (n-1)/2. In public key cryptography, two keys are used, one private key and other public key. Different keys are used for encryption and decryption. The private key is been used for decryption. The public key used for encryption and it available to the public. In each communication, new pair of public and private key is been created. It requires less no of keys as compared to symmetric key cryptography. Symmetric key is been used for long massage. Now discuss about some of the symmetric key management schemes in Ad-Hoc

3.1.1. Distribute key Pre-Distribution Scheme (DKPS)*:*

It consists of three important phases:

a) Distributed Key Selection (DKS) – In these phase every node takes the Random key from the universal set by using exclusive property.

b) Secure Shared-key Discovery (SSD) – In the second phase of DKPS in which every node having a shared key with another node. Node cannot find that which key on the ring are in common with which node. This method is not providing security, but easy to evaluate due to eavesdropping can occur in DKS phase.

c) Key Exclusion Property Testing (KEPT) - Last phase of DKPS symmetric key management scheme is KEPT. In its matrix is used for present the relationship between mobile nod‘s key and shared keys it uses binary values for constructing the matrix. A KEPT phase test that is all keys of mobile nodes fulfilling the exclusive property of CFF. Features of DKPS are no need of TTP. DKPS needs less storage as compared to pair-wise key agreement approach. This scheme is more efficient as compared to group key agreement [5]

3.1.2. Peer Intermediaries for Key Establishment (PIKE):

In this uses the sensor nodes to establish the shared key. PKIE is a symmetric key agreement scheme, it uses unique secret key in a set of nodes .This model uses the concept of random key pre-distribution, and in 2-D case with each of the O (n) nodes every mobile node shares a unique secret key in horizontal and vertical dimension. This scheme can extended to 3D or any other dimension. Features of this model are good security services, and fair scalability [6] .

3.1.3. Key Infection (INF):

This model is simple and every mobile node participates equally to making the key establishment process. INF model has no need of collaborative effort due to node acts as a trust component; this component broadcasts their symmetric key. This model is having weak security services, but INF having low storage cost, low encryption, and low operation. It has fair scalability with the problem of late entry of mobile node [7].

3.2 Asymmetric key management in Ad hoc Network

Asymmetric keys use two-part public and private key. Each recipient has a private key that is kept secret and a public key that is used for everyone. The sender sends the recipient’s public key and uses it to encrypt the message. The recipient uses the private key to decrypt the message and never publishes or transmits the private key to anyone. Thus, the private key is never passing over and remains invulnerable. This system is sometimes using public keys. This reduces the risk of data loss and increases compliance management when the private keys managed properly.

3.2.1 Secure Routing Protocol (SRP):

This scheme is been composed with three nodes and an administrative authority, which work as dealer in this model. Dealer is the entity, which provides the initial certificate to the mobile nodes. Three nodes are defined as: 1. Client Node. 2. Server Node. 3. Combiner Node. SRP node plays the important task in SRP model.

3.2.2 Ubiquitous and Robust Access Control (URSA):

URSA is efficient and provides reliable Availability with having the feature of encrypted local communication. This model uses efficient threshold scheme to broadcast the certificate (RSA Certificate) signing keys to all nodes. Each mobile node of Ad-Hoc updates their certificates periodically. This scheme provides communication delay, search failure, and degrades the system security. To protect the network from

DOS attack and the compromise the signing key URSA using verifiable and proactive secret sharing mechanisms [10].

3.2.3 Mobile Certificate Authority (MOCA):

The mobile nodes having great computational power, physically more secure. When the nodes are equally equipped than, MOCA nodes are selected randomly. This scheme is decentralized and the services of a CA are distributed to MOCA nodes [11]. In their scheme , a node could locate k+α MOCA node either randomly through the shortest path in its route cache .But the critical question is how nodes can discover those paths securely since most routing protocols are based on the establishment of a key services[11].

3.2.4 Partially Distributed Threshold CA Scheme:

Partially Zhou, L. and Hass, Z. discovered Distributed Threshold CA Scheme in 1999. When the mobile ad-hoc network is constructed, this scheme is using the concept of CA distribution in threshold fashion. Security services like off line authentication, great intrusion tolerance, and trust management by CA (certification authority) are provided by asymmetric key management scheme. The key is generated by this model are accepted by self-organized network and partial distributed threshold CA. This scheme is having the scalability of CRL (certificate revocation list), and certification [12].

3.2.5 Self-Organized Key Scheme (SOKS):

In the self-organized network each mobile node acts as a distinct CA.SOKS was disclosed by Capkun, S., Buttya, L., and Hubaux, P. in 2003. It has poor scalability and poor resource efficiency, but having the off line authentication and limited intrusion detection security services. SOKS having high intermediate encryption operations and high storage cost [13].

3.2.6 Key Distribution Technique (ID-C):

In this scheme node create or initialize the Ad-Hoc network with using the threshold private key generator identity based scheme. The generated key is been accepted by self-organized network. Off net authentication, trust management and intrusion tolerances type security services provided by ID-C asymmetric key management scheme. Scalability is been provided through an Id Revocation list with greater resources efficiency. This scheme has medium storage coast, operation and encryption [14].

3.2.7 Identity-Based Key Asymmetric Management Scheme:

In Secured ID-based key management scheme for Ad-Hoc network which allows nodes to use their public keys directly from their known network identities and with some other common information. This scheme provides inline Certification Authority (PKI) to share a secret key. It also provides end-to-end authentication and enables mobile user to ensure the authenticity of user of the peer node. The significant advantage of solution is to avoid users to generate their own public keys and then distribute these keys throughout the network. This scheme solved the security problem in the ad hoc network and it is suitable for application to other wired and wireless network. In this author mentioned major problem of security [15].

3.2.8 Three Level Key Management Scheme:

Secure and Wan AnXiong, Yao Huan Gong in 2011, proposes Highly Efficient Three Level Key Management scheme for Ad-Hoc network. To achieve three level security in ad hoc this model uses ID-Based Cryptography with threshold secret sharing, Elliptic Curve Cryptography (ECC) and Bilinear Pairing Computation. ECC provides short keys to mobile nodes and high security level. Key generation and key distribution security services in the prevention from adversaries attack has executed by (t, n) threshold secret sharing algorithm. ECC provides an enhanced security level with using 160 bits key and 1024 bits equivalent strength of RSA. Pairing technology provides confidentiality and authentication with less computational cost and reduced communication overhead [16].

IV. Comparative Survey

In the Previous Section we have discussed about some of the most important Key Management Techniques in Mobile ad hoc networks. In Comparative survey, we are going to compare these Key Management techniques based upon some of the Features like Reliability, Security, Scalability and Robustness. The Comparative Survey is made depending upon the results that are analyzed from various research works and journals. Table I shows the Comparative Survey of Key Management schemes in ad hoc Networks. Let us discuss about the features of Key Management schemes that we are going to compare.

4.1 Security*:*

Central security issues are trust management and vulnerability. Trust relations may change during the network lifetime. The system should enable the exclusion of compromised nodes. In order to judge the security of a key-management scheme, possible vulnerabilities should be important. Security services enabled one or a combination of confidentiality, integrity, authentication and non-repudiation.

4.2 Scalability:

Key management operations should finish in a timely. The fraction of the available bandwidth occupied by network management traffic should keep as low as possible. Any increase in management traffic reduces available bandwidth for payload data accordingly. Hence, scalability of key-management protocols is essential.

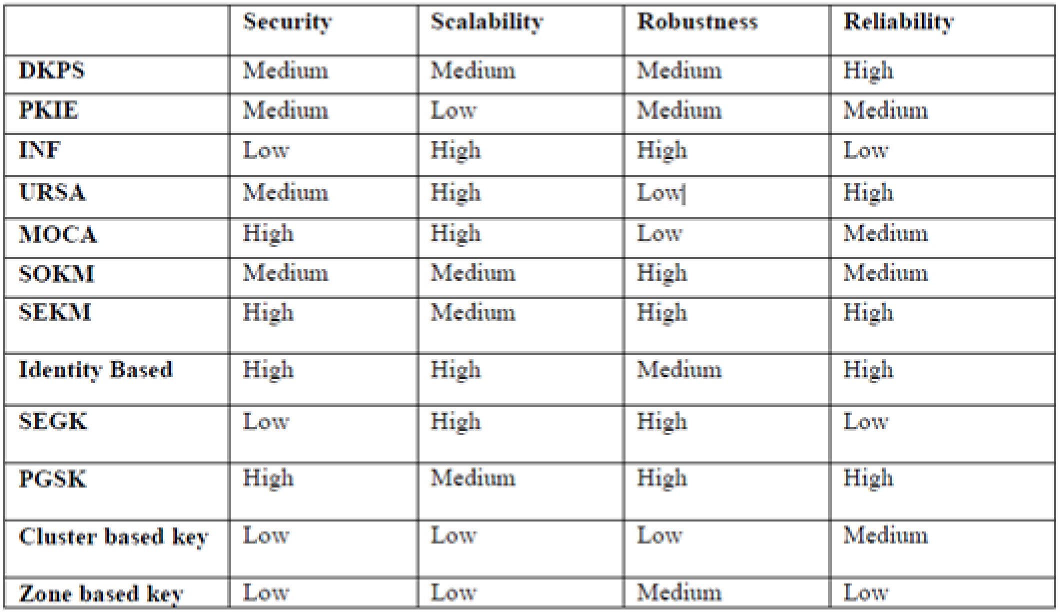
4.3 Reliability:

The Reliability of a Key Management scheme depends upon the Key Distribution, Storage and Maintenance. It is necessary to make sure that the Keys are Properly Distributed among the nodes, safely stored where hacker aren't able to hack the keys and should be Properly Maintained.

4.4 Robustness:

The key-management system should survive despite denial-off service attacks and unavailable nodes. The key-management operations should be able to be complete despite faulty nodes and nodes exhibiting behavior, that is, nodes that deliberately deviate from the protocol. Necessary key management operations caused by dynamic group changes should execute in a timely manner. Key management operations should not require network wide and strict synchronization. It is resistance to security attacks (e.g. man-in-the-middle).

TABLE1. Comparative survey of key management



	Security	Scalability	Robustness	Reliability
DKPS	Medium	Medium	Medium	High
PKIE	Medium	Low	Medium	Medium
INF	Low	High	High	Low
URSA	Medium	High	Low	High
MOCA	High	High	Low	Medium
SOKM	Medium	Medium	High	Medium
SEKM	High	Medium	High	High
Identity Based	High	High	Medium	High
SEGK	Low	High	High	Low
PGSK	High	Medium	High	High
Cluster based key	Low	Low	Low	Medium
Zone based key	Low	Low	Medium	Low

V. Conclusion

Different types of key management schemes covered in this survey paper. In summary, symmetric key management schemes described in three categories DKPS, PIKE and INF. DKPS symmetric key management scheme is much efficient as compared to group key schemes and pair wise key agreement. PIKE scheme has good security services with fair scalability. INF model has no need of a collaborative effort with having low storage cost. In this paper observe that DKPS is highly secure and efficient schemes as compared to other symmetric key management schemes. The identity-based key management is reliable. This scheme solved the security problem in the ad hoc network and it is suitable for application to other wired and wireless network. This is a major problem of security in the identity-based key management. SEGK is group key scheme in Ad-Hoc network double multicast tree is been constructed in this model. Two detection methods have introduced into SEGK scheme. Cluster based &Zone based key schemes come in hybrid or composite key management scheme. In future work, we will focus in Identity based secure key management using Elliptic Curve Cryptography. Advantages of using elliptic curve they seems to offer a level of security comparable to classical that use much larger key size .Minimum key sizes for ECC should be 132 bits Vs. 952 bits for RSA .

Acknowledgements

Author is thankful to his guides Mr. Anuj singh and Ms. Anuradha who give him an opportunity to carry out this work. Author is also thankful to NPTEL which provides E-learning through online Web and Video courses in Engineering, Science and humanities streams.

References

[1]. Panagiotis Papadimitraos and Zygmunt J. Hass, Securing Mobile Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 31), CRC Press LLC, 2003.
[2]. J.Kong P.Zerfos H.Luo, S.Lu and L. Zhang, “Providing robust and ubiquitous security support for mobile ad hoc networks”, in Proceedings of the 9th International Conference on Network Protocols(ICNP), November 2001, pp. 251-260.
[3]. Preetida Vinayakray-Jani,” Security within Ad hoc Networks”, Nokia Research Center, Helsinki, Finland. Position Paper, PAMPAS Workshop, Sept. 16/17 2002, London.
[4]. Wu, B., Chen, J., Wu, J., and Cardei, M. (2006). A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks. Wireless/Mobile Network Security, Springer. Chapter 12.
[5]. Aldar C-F. Chan, “Distributed Symmetric Key Management for Mobile Ad hoc Networks”, IEEE, 2004.
[6]. Aziz, B., Nourdine, E. and Mohamed, E., “A Recent Survey on Key management Schemes in MANET”ICTTA’08, pp. 1-6, 2008.
[7]. R. Anderson, Haowen and Perring, Adrian, “Key Infection: Smart trust for smart dust”, 12th IEEE International Conference on Network Protocol ICNP, 2004.
[8]. Valle, G. and Cerdenas, R., “Overview the key Management in Ad Hoc Networks”, ISSADS pp. 397 – 406, 2005.
[9]. Wu, B., Wu, J., Fernandez, E., Ilyas, M. and Magliveras, S., “Secure and Efficient key Management in mobile ad hoc networks”, Network and Computer Applications, Vol. 30, pp. 937-954, 2007.
[10]. Luo, H. and Lu, S., “URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks”, IEEE / ACM Transactions on Networking Vol. 12, pp. 1049-1063, 2004.
[11]. Yi, S., Naldurg, P. and Kravets , R, “Security-aware ad hoc routing for wireless networks ”,MobiHoc, pp. 299-302, 2001.
[12]. Zhou, L. and Hass, Z.,”Secure Ad Hoc Networks”, IEEE Network Magazine vol. 13, no. 6, pp.24-30, 1999.
[13]. Capkun, S., Buttya, L., and Hubaux, P.,”Self-Organized Public Key Management for Mobile AdHoc Networks”, IEEE Trans. Mobile Computing, vol. 2, no. 1, pp. 52-64, 2003.
[14]. A. Khalili, Katz, Jonathan and Arbaugh, William A.,” Towards secure key distribution in truly ad hoc networks”, IEEE Workshop on Security and Assurance in ad hoc Networks – i conjunction with the 2003 International Symposium on Application and the Internet, 2003.
[15]. AnilKapil and SanjeevRana, “Identity-Based Key Management in MANETs using Public Key Cryptography”, International journal of Security, vol. (3): Issue (1).
[16]. Wan AnXoing, Yao Huan Gong, “Secure and Highly Efficient Three Level Key Management Scheme for MANET”, WSEAS TRANSACTIONS on COMPUTERS, Vol. 10, Issue 10, 2011.
[17]. Bing Wu, Jie Wu and YuhongDong,”An efficient group key management scheme for mobile ad hoc network”, International Journal and Networks, Vol. 2008.
[18]. D. Boneh, X. Boyen, and H. Shacham, “Short group signatures,” in Advances in Cryptology–Crypto’04, Lecture Notes in Computer Science, vol. 3152, 2004, pp. 41–55.