International Journal of Advanced Technology in Engineering and Science
Vol. No.3, Special Issue No. 01, September 2015
www.ijates.com
ijates
ISSN 2348 - 7550

A MODIFIED APPROACH ON IDENTITY BASED CRYPTOGRAPHY AND DIGITAL SIGNATURE IN MANET

Er. Sonia Thakur[1], Er.Heena[2]

[1]*Research Scholar, CEC Landran*

[2]*Asstt.Prof. I.T. Deptt.CEC Landran*

ABSTRACT

A Mobile Ad Hoc Network (MANET) is defined as the group of wireless mobile nodes that forms a temporary network without using existing network infrastructure or administration. Identity-based encryption (IBE) is an encryption technique of public key encryption in which user is able to identify the keys that are already replaced. Decryption key is given to every user as a secret key to decrypt the message and encryption key is also provided to the every user to keep his identity hidden from others or from attacker. Here, the combination of Digital Signature and IBE is to be used to share the data with keeping the identity of the node in the network hidden.

Keywords: MANET's, IBC, PKI, PKG, CA, DSA

I. INTRODUCTION

Both in academia and industry the research on MANETs security remains active as the research is being done since from many years. It is partially due to the fact that no other option is widely accepted and the growing availability of small, personalized mobile devices with peer to peer communication capability through wireless channels. There are my measures in security requirements for MANETs that include are as follows are data confidentiality, data integrity, data freshness, data availability, Data & Identity Authentication and non repudiation [1]. Data Confidentiality is allows to keeps the data secret to outsiders, Data Integrity is that which prevents the data from being altered or prevents from any modification done by attacker, Data Freshness is defined as that it keeps the data in the right order and updated, Data Availability allows to ensures that the data is available when any user is demand on request, Data & Identity Authentication is used to verifies the data or request came from a valid sender, and non-repudiation is used to ensures a node that cannot deny sending a message. Security mechanisms basically used as mechanisms that are widely involved and proven to be effective in wired networks but it may be not always applicable to MANETs. Attacks that can be easily or can be detected very fast or in less time and can be prevented in wired networks have a big security challenges in MANETs networks. There are many Examples that include, but they are not that much limited to identity/address spoofing, message tampering and forgery, message replay, etc. If compared to wired networks,

the combination of the following list of characteristics of MANETs makes it especially difficult to achieve security requirements:

- There is lack of network infrastructure and online administration.
- Network topology and node membership dynamics.
- The potential insider attacks

  In the early research many problem are come across the path of Security proposals that the attack can be done easily. As we are entered into the modern world there are many techniques that are used to protect the private data from the attackers. It is hard for the attacker to find the private or confidential data with the help of new techniques and policies. Some protocols are also made or designed for the limited attack models, but may collapse under combined or unanticipated attacks [2]. Cryptography is a technique that is used to design a basic framework. Cryptography techniques that are used in MANETs can be divided into two types that are namely as first as Symmetric Key based and Asymmetric Key based. When talk about symmetric key based schemes, in symmetric key based technique the same key is used by the sender and the receiver to send the message. If an attacker knows the symmetric key that are used by the group of users, then all encrypted messages for that group will be known to the attacker very easily and the attacker is able to change the message. In the case of Asymmetric key based schemes it uses the different key to encrypt or decrypt the message that is send by the sender to the receiver and can be provide more secure and have many functionalities than symmetric ones, e.g., key distribution is much easier, authentication and non-repudiation are available, compromise of a private key of a user does not reveal messages encrypted for other users in the group. However, they are generally more costly. Traditional asymmetric cryptography is one of them in which it is widely and effectively based on Public Key Infrastructure (PKI) which deals with internet. Certificate Authority (CA) is used in PKI used as or depend on the availability and security.CA is a authority that is trusted by every user in the network. Another problem or we can say a disadvantage with the PKI is that in MANET there is problem for saving and transmit the overhead of public key certificates (PKCs). Identity-based cryptography (IBC) is a special form of public key cryptography. IBC remove the requirement of CA and PKCs. Since 2001, IBC has attracted more and more attention from security researchers. Some properties of IBC make it especially suitable for MANETs. Fang et al. [3], [4] that can be explained by the advantages of IBC that are as follow:-
- Easier to deploy without any infrastructure requirement. This saves certificate distribution, while bringing ―free pair wise keys without any interaction between nodes.
- Its resource requirements, regarding process power, storage space, communication bandwidth, are much lower.
- The public key of IBC is self-proving and can carry much useful information.

  When we are come across the survey on the security application in MANET From 2001 to 2010 it shows many properties of the IBC. It also shows the problems or disadvantages that are come across the path of the research. Since difficulty of MANET security lies on differences between MANETs and wired infrastructure networks in network and lower layers, identity-based cryptosystems are mostly employed in network layer, i.e. in routing protocols.

II. SECURITY FACTORS

AUTHENTICATION: Authentication enables a MANET to ensure the identity of the peer node it is communicating with. Without authentication, an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes.

NON-REPUDIATION: It ensures that the original message cannot deny having sent the message. Non-repudiation is useful for detection and isolation of compromised MNs. Ensures that sending and receiving parties can never deny ever sending or receiving the message.

CONFIDENTIALITY: Confidentiality ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, such as strategic or tactical military information, requires confidentiality.

KEY AND TRUST MANAGEMENT: Key and trust management is a critical supporting element in any security systems. Its basic operations include establishing key exchange and update, as well as secret connections. Keys are the basic blocks of symmetric and asymmetric cryptographic functions, which in turn furnish authentication, confidentiality, integrity, and non-repudiation security services. The main body of key and trust management in MANETs is concerned with a hybrid of asymmetric and symmetric cryptosystems, where trust is established via credential verification, and shared secrets are exchanged for latter use in efficient symmetric cryptosystems. An inherent issue in trust management is the trust graph, where the MNs correspond to the network entities and edges to the verifiable credentials. The security in networking is in many cases dependent on proper key management. Key management consists of various services, of which each is vital for the security of the networking systems.

Trust model: it must be determined how much different elements in the network can trust each other. The environment and area of application of the network greatly affects the required trust model. Consequently, the trust relationships between network elements affect the way the key management system is constructed in network.

Trust third party (TTP): [8] a centralized authority (e.g., a key distribution center [KDC] or certification authority [CA]) is trusted by every entity and an entity A is trusted by another if the authority claims A is trustworthy. This schemes is centrally managed, thus the neighborhood of the central point is potentially the bottleneck of a scalable network and subject to DoS attacks.

Web-of-trust: There is [9] no particular structure exists in such trust graphs. Each entity manages its own trust based on direct recommendation from others. The scheme is fully distributed, making it resilient to attacks, but also difficult to achieve consensus among various entities.

Localized trust: [10] this model is the middle ground of the previous two graphs. A node is trusted if any k trusted entities among the node's one-hop neighbors claim so, within a bounded time period. As trust management and maintenance are fully distributed in space and time domains, the model fits in large dynamic ad hoc networks with mobility and on-demand authentication requirements.

Cryptosystems: available for the key management: in some cases only public-or symmetric key mechanisms can be applied, while in other contexts Elliptic Curve Cryptosystems (ECC)are available. While public-key cryptography offers more convenience (e.g. by well-known digital signature schemes), public-key cryptosystems are significantly slower than their secret-key counterparts when similar level of security is

needed. On the contrary, secret-key systems offer less functionality and suffer more from problems in e.g. key distribution. ECC cryptosystems are a newer field of cryptography in terms of implementations, but they are already in use widely, for instance in smart card systems.

III. RELATED WORK

Identity-based cryptography is a specific instance of open key cryptography that in specific conditions offers execution and usage focal points, without decreasing the security degree. In an ordinary open key security plot, the era of the two keys (the private key and general society key) begins from a capricious arbitrarily picked expansive number. This prompts two irregular keys numerically limited. Given the irregular character of the general population key, it can't be given as is to the intrigued clients in light of the fact that it would be exceptionally hard to store and to utilize. That is the reason the testaments are utilization to tie the way to the client and to the issuing accreditation power. The need of the authentications decides, before any correspondence, the need to hunt down the qualified endorsement of the individual somebody might want to safely speak with and to accept this declaration to verify that it has a place with the other party. Be that as it may, imagine a scenario in which people in general key can be picked.

This is the determinant normal for personality based cryptography (IBC): the general population key is no more irregular, yet a bit of data with respect to the character of the client [1]. For instance, the entire name, the email location or the personal residence can all be use as an open key. The picked data ought to consent to a few guidelines like: the data ought to be extraordinarily bound to a client, the data ought to be bound in a manner that the clients can't later deny, and, obviously, this data ought to be openly accessible. In this paper we will introduce the general hazardous of character based cryptography, with an accentuation on its conceivable applications, particularly in military associations. Whatever remains of the paper is composed as takes after. The second area introduces the numerical foundations of personality based cryptography

Qualities of character based cryptography: The clients of a personality based cryptography plan can infer their open key beginning from the estimation of a character component, which, more often than not, is an ASCII esteem [1]. After the general population key is picked, the comparing private key must be produced. In the event that a client could produce they claim private key for people in general key they have picked, then they could create the private key for whatever other client of the same security plan, on the grounds that the general population keys are open. In the event that this would happen, the security would be bargained. That is the reason the private key must be created by an exceptionally assigned key era focus (KGC). The KGC has likewise a couple of keys: an open and a private one. Beginning from the character of a client (which is additionally the client's open key) and utilizing its private key, the KGC processes the private key of each client. From a scientific perspective, personality based cryptography is a specific type of blending based cryptography. The IBC cryptosystem is fabricate taking into account blending between components of a gathering to a second gathering. The blending can be viewed likewise as a mapping from components from the first gathering to components from the second gathering. Along these lines, a hard issue in one gathering is decreased to a less demanding issue in the other. A character based cryptographic plan comprises out of four calculations [2]:

• Setup calculation is run stand out time by the KGC. In this stride the private and open key pair of the KGC is made alongside the others parameters of the plan.

• Key era calculation is controlled by the KGC for each client that requests its private key. The outcome is the private key of this client and it is transmitted to it.

• Encryption calculation utilizes the personality of a hub (its open key) to scramble a message for this hub.

• Decoding step is performed at the getting hub: utilizing its private key the hub unscrambles the scrambled message and acquires the reasonable message.

Other than these four calculations, others perspectives ought to be contemplated. At the point when a client requests a private key, the KGC must verify the client to make certain that they are not mimicking another so as to figure out they private key. On the off chance that the confirmation succeeds, the private key must be transmitted to the client on a protected divert with a specific end goal to abstain from spying by a vindictive client ([3]).

IV. BASIC CONCEPTS OF IBE AND SIGNATURE

In this area we examine the prerequisites of the Identity based encryption and Identity based signature

A. Identity based signature: As specified prior, in the IBE plan, the sender Alice can utilize the collector's identifier data which is spoken to by any string, such email address, IP addresses, government managed savings number, a photograph, a telephone number, postal location and so on., to encode a message. The recipient Bob, having acquired a private key connected with his personality data from trusted outsider called the "Private Key Generator (PKG)", can unscramble the cipher text.

Summing up, we portray an IBE plan utilizing the accompanying steps.

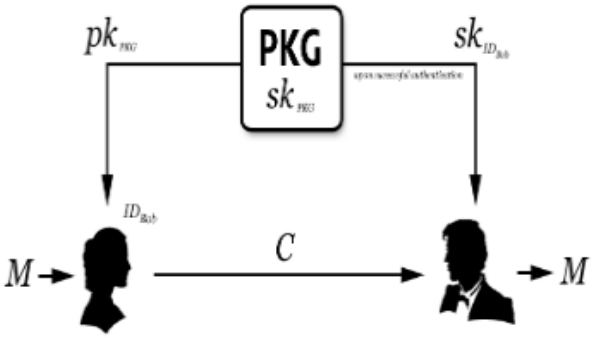

Figure 1: Schematic outline of an IBE scheme

Setup: The PKG creates its master (private) and public key pair, which we denote by skPKG and pkPKG respectively. (Note that pkPKG is given to all the interested parties and remains as a constant system parameter.)

Private Key Extraction: The receiver Bob authenticates himself to the PKG and obtains a private key skid Bob associated with his identity ID Bob.

Encryption: Using Bob's identity ID Bob and the PKG's pkPKG, the sender Alice encrypts her plaintext message M and obtains a cipher text C.

Decryption: Upon receiving the cipher text C from Alice, Bob decrypts it using his private key skID Bob to recover the plaintext M.

B. **Identity based signature.** As a mirror image of the above identity-based encryption, one can consider an identity-based the signature (IBS) scheme. In this scheme, the signer Alice first obtains a signing (private) key associated with her identifier information from the PKG She then signs a message using the signing key. The verifier Bob now uses Alice's identifier information to verify Bob's signature.

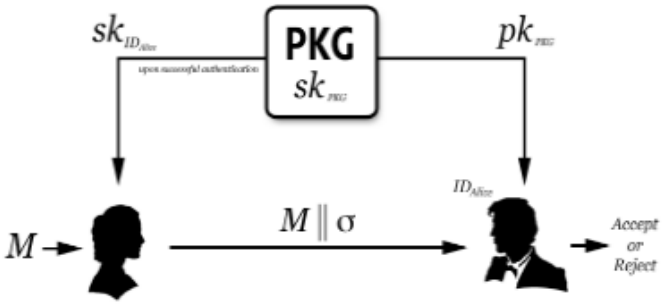

Figure 2: Schematic outline of an IBS scheme.

No needs for Bob to get Alice's certificate. More precisely, an IBS scheme can be described using the following steps.

Setup: The Private Key Generator (PKG),which is a trusted third party, creates its master (private) and public key pair, which we denote by skPKG and pkPKG respectively.

Private Key Extraction: The signer Alice authenticates herself to the PKG and obtains a private key skID Alice associated with her identity ID Alice.

Signature Generation: Using her private key skID Alice, Alice creates a signature σ on her message M.

Signature Verification: Having obtained the signature σ and the message M from Alice, the verifier Bob checks whether σ is a genuine signature on M using Alice's identity ID Alice and the PKG's public key pkPKG. If it is, he returns “Accept". Otherwise, he returns “Reject".

V. RESULTS

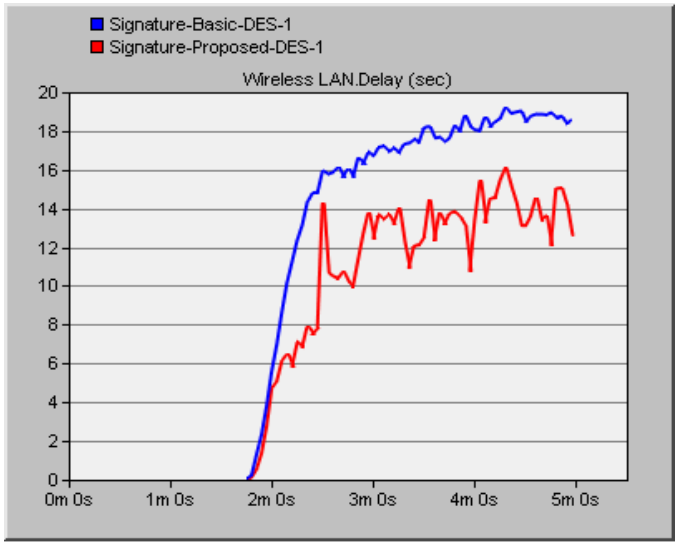

Figure 3: Delay

Figure 4 defined about the delay possessed by the existing and proposed approach. Proposed approach has much lesser delay than that of existing one.

ijates
ISSN 2348 - 7550

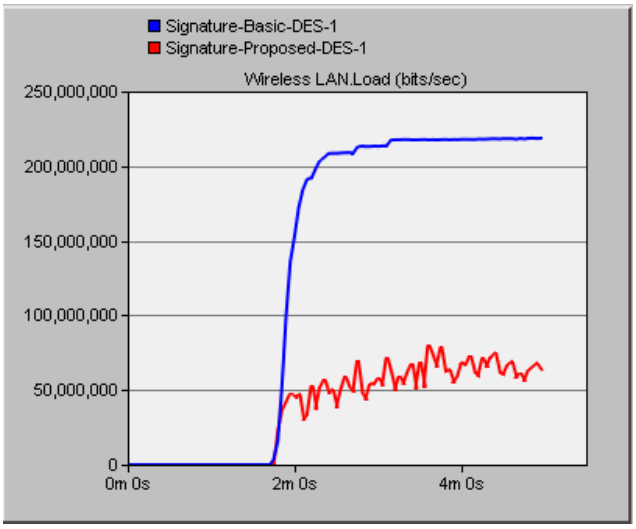

Figure 4: Load

Load defined in figure 5 is quite better in case of proposed system as compared to the Existing.

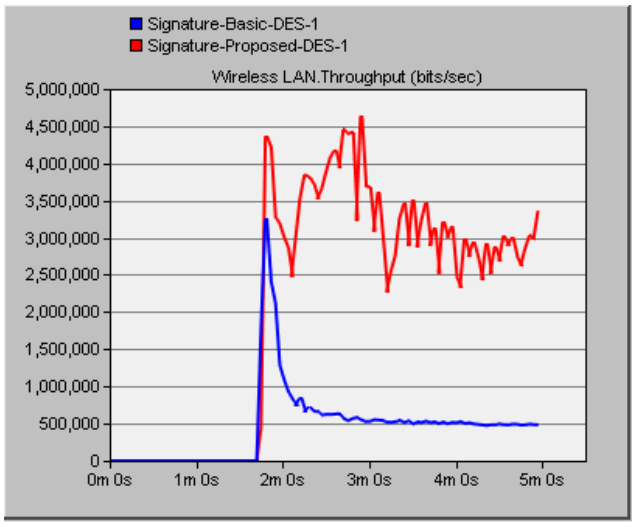

Figure 5: Throughput

Throughput in the proposed approach is lower than that of existing approach.

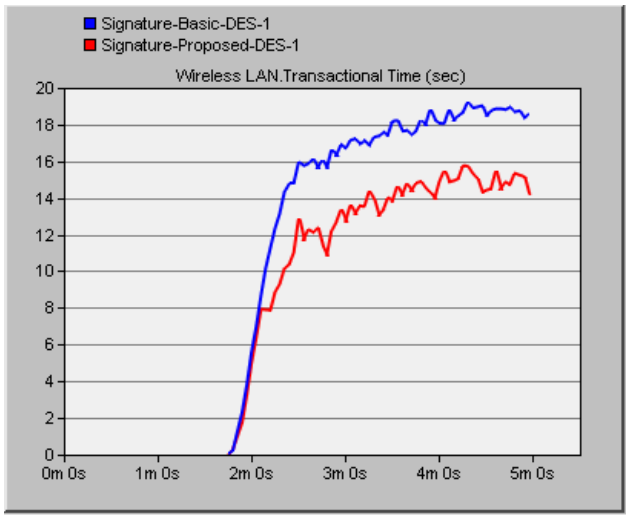

Figure 6: Transactional Time

This figure shows that the transactional time means encryption and decryption time is less in case of proposed scenario.

VI. CONCLUSION

It is clear that the security aspects related to ad hoc networks form a very complex problem fields, given the dynamic and unpredictable nature of most ad hoc networks. On the other hand, ad hoc networks vary from each other greatly from the viewpoint of the area of application. Some ad hoc networks may not need security solutions other than simple encryption and username-password authentication scheme. All security mechanisms applied in networking more or less require the use of cryptography, which on the other hand implicates a strong demand for secure and efficient key management mechanism. Access control needs to exist a method for restricting the access of foreign nodes to the network, which requires the use of a proper authentication mechanism. On one hand, the security-sensitive applications of ad hoc networks require high degree of security; on the other hand, ad hoc networks are inherently vulnerable to security attacks. Therefore, security mechanisms are indispensable for ad hoc networks. The idiosyncrasy of ad hoc networks poses both challenges and opportunities for security mechanisms.

REFERENCES

[1] Jayraj Singh, Arunesh Singh, Raj Shree "An Assessment of Frequently Adopted Security Patterns in Mobile Ad hoc Networks: Requirements and Security Management Perspective, Journal of Computer Science and Data Mining ,Vol. 1,No. 1-2,December 2011

[2] Stallings W [2000], Network Security Essentials: Security Attacks. Prentice Hall. (pp. 2-17).

[3] Hao Yang, Haiyun Luo, Fan Ye, songwu Lu and Lixia Zhang,"Security in mobile ad hoc networks: Challenges and solutions", IEEE Wireless Communications, Vol. 11,(2004) pp. 38-47.

[4] Hoang Lan Nguyen, Uyen Trang Nguyen "A study of different types of attacks on multicast in mobile adhoc networks", Journal of Ad hoc Networks, Vol. 6,(2006),pp. 32-46.

[5] Sudhir Agarwal,Sanjeev Jain, sanjeev Sharma,"A survey of Routing attacks and security Measures in mibile adhoc networks",Journal of computing , Vol 3, Issue 1,(2011), pp. 41-48.

[6] Bing Wu, Jianmin Chen,Jie Wu, Mihaela cardei ,"A survey on Attacks and Countermeasures in Mobile ad hoc networks",Wireless/Mobile network security, Springer,(2006).

[7] Manel Guerrero Zapata, N. Asokan in Nokia research center and was submitted to WiSe'02, September 28, 2002, Atlanta, Georgia, USA".

[8] Kimaya Sanzgir, Bridget Dahilly, Brian Neil Levine, Clay Shields, Elizabeth M and Belding-Royer [2002]. "A Secure Routing Protocol for Ad Hoc Networks". Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP'02).

[9] Yih-Chun Hu, David B. Johnson and Adrian Perrig. "Secure Efficient Ad hoc Distance vector routing" in the Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and applications (WMCSA'02).

[10] Adrian Perrig, Ran Canetti, Dawn Song, and J. D. Tygar. Efficient and Secure Source Authentication for Multicast. In Network and Distributed System Security Symposium, NDSS '01, pages 35–46, February 2001.

[11] Ping Yi, Zhoulin Dai, Yiping Zhong, Shiyong Zhang [2005]. "Resisting Flooding Attacks in Ad Hoc Networks". Proceedings of the IEEE International Conference on Information Technology: Coding and Computing (ITCC'05).

[12] Anand Patwardhan, Jim Parker and Anupam Joshi. "Secure Routing and Intrusion Detection in AdHoc Networks". [On-line] accessed on 6th November, 2005 at URL http://csrc.nist.gov/mobilesecurity/ Publications/ nist-umbc-adhocids-ipv6.pdf.

[13] Panagiotis Papadimitratos and Zygmunt J. Haas In Proceedings of the SCS Communication Networks and Distributed Systems Modelling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002.

[14] Basagni, S. Conti, M. Giordano, S. Stojmenovi & cacute (Edition). [2004]. Mobile Ad Hoc Networking: September 2004 Wiley-IEEE Press. (pp. 1-33, 275-300, 330-354) C. Siva Ram Murthy and B.S. Manoj. [2004]. Ad Hoc Wireless Networks, Architecture and Protocols: 2004 Pearson Education (pp. 321-386, 473-526).