SECURE DATA PACKET TRANSMISSION IN MANET USING ENHANCED IDENTITY-BASED CRYPTOGRAPHY (EIBC)

P.Subbulakshmi[*] and S.Vimal[$]
[*]Assistant Professor[$]Assistant professor (Senior Grade), Department of Information Technology,
National Engineering College, Kovilpatti, Tamilnadu, India.

***Abstract*— Mobile ad hoc network (MANET) is a self configuring and self relating wireless network of mobile nodes connected devoid of wires. Due to their unique characteristics such as mobility, dynamic topology and lack of essential infrastructure support, security is more challenging in MANET. So, to enhance the security in MANET, we propose Enhanced Identity-Based Cryptography (EIBC), an efficient key management mechanism uses cryptography concept for encryption and decryption of data packets beside with routing information. EIBC system has secret values which perform similar to the original model secret value. In EIBC, the node calculates the live public key and live private key for verification purpose. Enhanced ID-Base Signature is also used for authentication rationale using signature. After completing verification purpose, the protected channel sends the data packets using Enhanced ID-Based Encryption. In Enhanced ID-Based Encryption, the node sends the packet in an encrypted mode using live public key and the node receives the packet in a decrypted mode using live private key. EIBC achieves a elevated level of security while handling system key refreshment process in an efficient manner. The brute force attack is averted by constructing EIBC. The performance is analyzed when there is security mechanism and when there is no security mechanism.**

Keywords— Enhanced ID-Based Encryption, Enhanced ID-Base Signature,MANET, key refreshment,brute-force attack.

1. INTRODUCTION

In MANET, nodes are mobility in environment and it has no predetermined infrastructure [1]. Nodes in ad hoc network proceeds as routers which causes network layer to be more susceptible to security attacks.The great challenges of MANETs are their vulnerabilities to assorted security attacks [2] and inability to maneuver securely while preserving its resources and achieve secure routing among nodes. So it is enormously essential to construct security mechanism to guarantee the secure path in MANET.

Mobility in MANET leads to lack of numerous security measures, which is used in conventional wireless network with the fixed infrastructure. Security proposals in early research are characteristically attack oriented. They often first identify several security threats and subsequently enhance the existing protocol or propose a new protocol to thwart them. Such solutions are devised explicitly against limited attack models. They exertion well in the occurrence of designated attacks but may collapse under pooled or unanticipated attacks [3].

However, compared with the wired network, the mobile ad hoc network will need supplementary robust security scheme to ensure the security of it. To overcome the vulnerabilities of ad hoc networks, the security

mechanism called Enhanced ID Based Cryptography (EIBC) is intended. The contribution of this paper is summarized as follows:

- Design a security mechanism baptized Enhanced Identity-Based Cryptography (EIBC) to provide the secure transmission between the nodes in MANET. It ensures the secure path by applying encryption and signature verification process in AODV protocol.
- EIBC can prevent the brute force attack by establishing a true link between the routes and nodes.
- It can greatly increase the packet delivery ratio and provide an improved facility to send the data packets in a secure manner.

The rest of the paper contains six sections. In Section 2, we summary related works and spotlight on the difference between our work and other related works. In Section 3, we construct a security mechanism in MANET to generate secret values, to send the secure data packets by applying encryption and signature verification process which is managed by bilinear pairing. In Section 4, we depict the key refreshment process to refresh the keys and the brute force attack is prevented by using this EIBC mechanism in AODV protocol. In Section 5, we show our simulation results to analyze the performance when there is security mechanism and when there is no security mechanism in the network environment. Finally, Section 6 presents the conclusion.

2.RELATED WORKS

K.Sangeetha et al., [4] proposed Elliptic curve cryptography (ECC) to provide secure data transmission in the network. Elliptic curve cryptography (ECC) can be developed in order to make the path more secure and also used to eliminate the requirement of pre-distributed keys. It is used to make the path more secure and also used to achieve high security level with smaller key size. The security of ECC is mainly due to difficulty of solving the elliptic curve discrete logarithm problem.

Shushan Zhao, Akshai Aggarwal et al., [5] discussed about the Identity Based Cryptography (IBC) for different applications in mobile ad hoc environment because security is not much ensured in MANET due to nature of its mobility. It is an approach to eliminate the requirement of a Certificate Authority (CA) and Public Key Certificates (PKC).The public key of IBC is self-proving and can carry much useful information. The interdependency cycle between secure routing and security services is addressed, but it is not efficient, because of communication and computational overhead of broadcast.

Abdul Manaf, Babak Emami et al., [6] developed Identity-Based Cryptography to generate the keys based on user's identity and to increase the authenticity performance. Identity-Based Cryptography (IBC), is a method that public key generated based on user's identity. Secured routing information used to transfer data from one node to another node is difficult task to sustain. Once node has been compromised, fake routing table can be distributed through the network and critical information through these compromised nodes can be easily trapped.

Craig Gentry and Alice Silverberg et al., [7] presented hierarchical identity-based encryption schemes and signature schemes that have total collusion resistance on an arbitrary number of levels and that have chosen cipher text security in the random oracle model. Authentication and private key transmission can be done locally. A HIDS adversary also has the ability to choose its target, and to make public key queries and private key extraction queries on entities other than the target and its ancestors. In this scheme, the user's ancestors can compute a different private key for the user based on different Q-values to forge the user's signature.

A.Kahate and V.Chandure et al., [8] proposed cryptography mechanism to detect selfish, malicious behavior of nodes and securing information from other types of attacks. The main advantage is to authenticate the node and ensure the security of important routing information. The malicious nodes try to disrupt network function by modifying packets, injecting packets or creating routing loops. It allows the attackers to influence the victim's selection of routes or enable the denial of service attacks.

R. Vedhavarshini and T. Anand, et al., [9] proposed Hybrid based cryptography to transmit the data packets in an efficient way and analyze the various Intrusion Detection System (IDS) to avoid packet data loss in network avoid routing overhead by deleting malicious node's route in MANET. Network overhead increases when number of malicious node in that network increases, because the count of acknowledged packet increases. It has disadvantages such as unwanted network overhead due to two acknowledgements used in every data packet sent and degrades network performance.

Anil Kapil and Sanjeev Rana et al., [10] proposed a secure identity-based key management scheme to focus the security problem in MANET and provides end-to-end authentication without any Public Key Infrastructure (PKI). It permits mobile nodes to derive their public keys directly from their known network identities. The significant advantage of proposed scheme is to avoid users to generate their own public keys and to then distribute these keys throughout the network. They did not find any efficient solution based on ID based key management scheme.

Vinayak & Nahala et al., [11] gives an idea of implementing a new encryption schema that will prevent a change of brute forcing in simple MANET single hock network. Honey encryption provides an efficient security against brute force attacks for some kind of messages. They didn't focus any signature scheme to ensure the security authentication by preventing brute force attack. The key of password attacker can use sophisticated tools to easily crack the hashes when the underlining passwords are weak.

Vanesa Daza, Javier Herranz, Paz Morillo et al., [12] analyzed some cryptographic techniques to securely set up a mobile ad-hoc network. The process is fully self-managed by the nodes, without any trusted party. They achieved decentralization and full dynamism as well as each node can obtain a pair of secret/public keys for its own use and the system can enjoy proactive security, which leads to a long-lived MANET. The standard secret sharing techniques makes dynamism but it is difficult to achieve.

R. K. Sharma, Neeraj Kishore et al., [13] presents a secured and efficient way of sending data and image in encrypted form using Identity Based Cryptography and Visual Cryptography. It has direct application in MANETs specifically for military surveillance. The initial function is to set up the base station / control room which contains the identity information of all the mobile nodes along with their public and private keys.

Shane Balfe, Kent D. Boklan et al., [14] introduces a lightweight and secure framework enabling the refreshing of private keys in identity based public key infrastructures. The use of multiple parameter sets is a requirement to support coalition forming and forward security is a nice security property but it seems difficult to achieve. The appearance of multiple public keys is an unfortunate inefficiency.

Hasaen Nicanfar and Victor C.M Leung et al., [15] proposed Enhanced Identity Based Cryptography (EIBC) to ensure the secure path in smart grid networks. It is an efficient key management mechanism that minimizes control packets communications. EIBC significantly reduces the number of required control packets for key management, which improves the efficiency of system resource utilization. They did not conclude any type of attack to prove the security. The performance is not analyzed for this security method.

In MANET, the security is provided by two ways: i) one to protect the data transmission and ii) to make the routing protocol secure. From these works, different security mechanisms are proposed to ensure the secure path. But, we propose an Enhanced ID- Based Cryptography (EIBC) to enhance the security by generating the keys itself and the brute-force attack is prevented by appending the security mechanism in AODV protocol.

3.ENHANCED ID BASED CRYPTOGRAPHY

In EIBC, first of all setup some values. Second, the keys will be generated with use of bilinear pairing. The bilinear pairing consists of the two groups such as additive group and multiplicative group. Then the public key is generated with use of hash function and node's id. But the private key is extracted with use of node's id, hash function and secret value. Then the keys will be exchanged between the sender

and receiver node for made the encryption and decryption process. After that, the signature will be generated and verified with use of its own keys. Finally, the keys are refreshed depends upon the time.

3.1 Setup values

The random value is selected first and with use of that random value, secret value is created. The random value is constructed with use of Pseudo Random Number Generator (PRNG) which contains two parameters such as A & B . These parameters are used for addition and modulo operations. And the periodic modification function is also constructed to concatenate the groups which are managed by bilinear pairing. Then the public key is generated by using the hash function and the node's id.

$$P_bK_A^i = H_1^i(ID_B) \quad (1)$$

where $P_bK_A^i$ refers to the sender's public key, H_1 refers to the hash function and ID_A refers to the sender's ID.

3.2 Private key extraction

The private keys are extracted from the secret value and its own id. In this step, the keys are verified with use of bilinear pairing which consists of communicative group and modulo group.

$$P_rK_B^i = l \quad (2)$$

$$\hat{e}(P_rK_B^i, P_I) = \hat{e}(h_i(s_i), s_i, H \quad (3)$$

where $P_rK_B^i$ refers to the receiver's private key, ê refers to the bilinear pairing, s_i refers to the secret value, P_I refers to the seed value of the key and ID_B refers to the receiver's id.

3.3Enhanced ID-Based Encryption (EIBE)

3.3.1Encryption:

When the sender wants to send a message to receiver, first sender calculates the live public key of the receiver using receiver's ID as below:

$$P_bK_B^i = H_1^i(ID_B) \quad (4)$$

where H_1 refers to the hash function, ID_B refers to the receiver's id and $P_bK_B^i$ refers to the receiver's public key.

Then the message is encrypted using random variable and receiver's public key

$$C = r.\tilde{P}_i, M \oplus H_2(P_bK_B^i) \quad (5)$$

where r is a random variable, M is a message to be encrypted and $\tilde{P}_i$ refers to the public key seed value.

3.3.2Decryption:

Receiver utilizes his own private key and decrypts the message as follows:

$$P_rK_B^i = h_i(\tilde{s}_i).H_1^i(ID_B) \quad (6)$$

$$M \oplus H_2\left(\hat{e}\left(PbK_B^i, P_i\right)^r\right) \oplus H_2\left(\hat{e}\left(PbK_B^i, P_i\right)^r\right) \quad (7)$$

where $P_rK_B^i$ refers to the receiver's private key, ID_B refers to the receiver's id, r refers to random variable and H_2 refers to the hash function.

3.4 Enhanced ID-Based Signature (EIBS)

3.4.1 Signature:

The sender uses H_3 value and calculates as its signature for the message M as follows:

where $P_rK_A^i$ refers to the sender's private key.

3.4.2 Verification:

Finally, the receiver verifies the signature using the equation as follows:

where ê refers to the bilinear pairing which consists of two groups such as additive group (G_1) and multiplicative group (G_2), where P_i refers to the public key seed value and $P_bK_A^i$ refers to the sender's public key.

4.KEY REFRESHMENT

EIBC has three timers such as Short-Term Refreshment (STR), Long-Term Refreshment (LTR) and Medium-Term Refreshment (MTR) to refresh the keys. The keys will be refreshed depends upon the time. In STR, the keys will be refreshed by using secret value and updates the hash function. In MTR, the random value is newly generated to refresh the private keys. In LTR, the keys will be refreshed by taking a large amount of time. For long term, the same keys will be used.

Finally, the brute force attack is prevented by using the cryptographic keys. Brute force attack means hack the username or password in a system and used against any encrypted data. The attacker cannot able to understand the encrypted message and the attacker node may not capture the keys and signature because it is verified itself before sending the message to another node. Therefore, the brute force attack is prevented by using the enhanced identity base cryptographic mechanism in MANET. For packet transmission, the AODV protocol is used and appended with the EIBC mechanism.

5.PERFORMANCE EVALUATION

Performance of the network can be evaluated through maximum speed changes in the network and metrics used in network. The following performance metrics are used for the evaluation. The following metrics are going to analyze after the detection of attacks and also after the prevention of security attack.

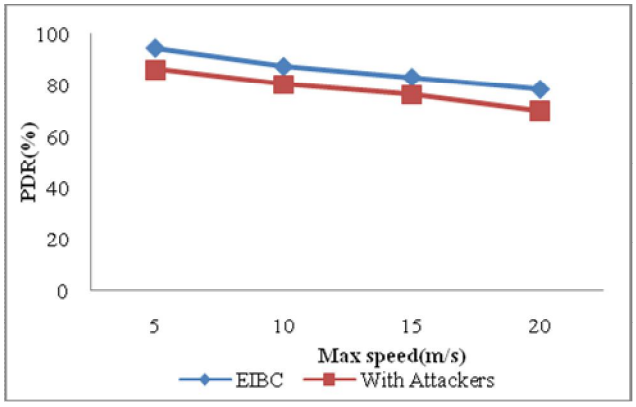


Figure 1: Max speed vs. PDR

From the graph, the x-axis is taken as the maximum speed which is measured in terms of metre per second. The y-axis is taken as packet delivery ratio which is measured in terms of percentage. When the maximum speed increases the packet delivery ratio is also increased. But when the attacker is detected and before prevented, the packet delivery ratio is decreased. Then compare it with after prevention, the security mechanism EIBC in AODV protocol produces a improved performances.

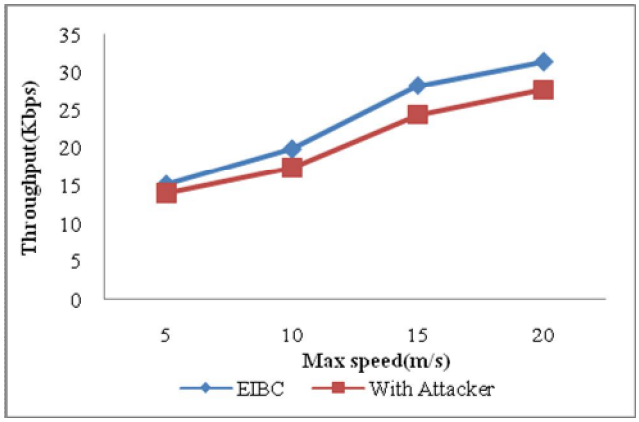


Figure 2 :Max speed vs. Throughput

From the graph, the x-axis is taken as the maximum speed which is measured in terms of metre per second. The y-axis is taken as throughput which is measured in terms of kilobits per second. When the maximum speed increases the throughput is also increased. But when the attacker is detected and before prevented, the throughput is decreased. Then compare it with after prevention, the security mechanism EIBC with AODV protocol produces better performances.

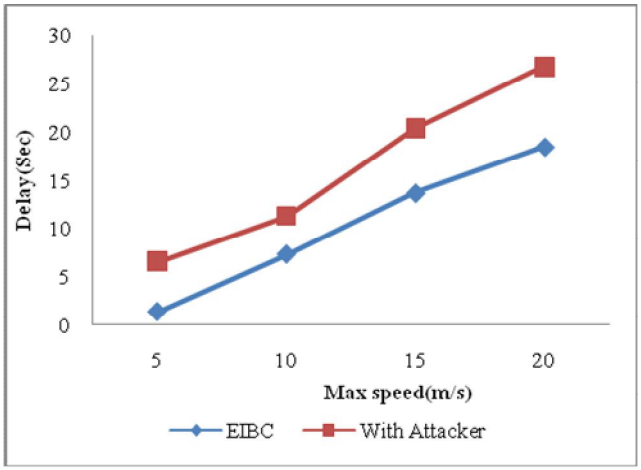
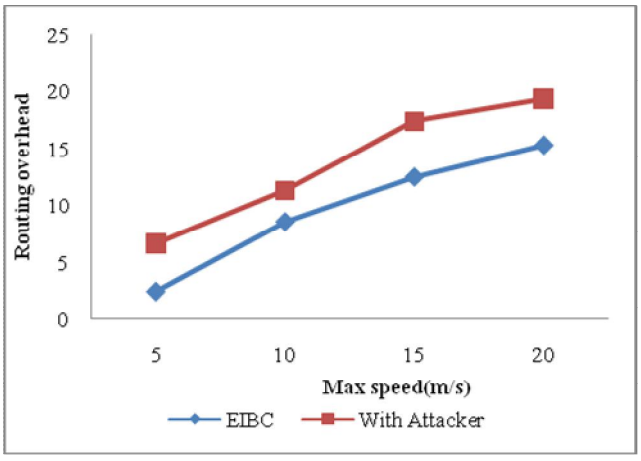


Figure 3: Max speed vs. End-to-End Delay

From the graph, the x-axis is taken as the maximum speed which is measured in terms of metre per second. The y-axis is taken as delay which is measured in terms of seconds. When the maximum speed increases the delay is decreased. But when the attacker is detected and before prevented, the delay is increased. Then compare it with after prevention, the security mechanism EIBC which is appended in AODV produces an enhanced performance.



Figurte 4 :Max speed vs. Routing overhead

From the graph, the x-axis is taken as the maximum speed which is measured in terms of metre per second. The y-axis is taken as routing overhead which is measured by packets. When the maximum speed increases the routing overhead is decreased. But when the attacker is detected and before prevented, the routing overhead is increased. Then compare it with after prevention, the security mechanism EIBC with AODV produces superior performances.

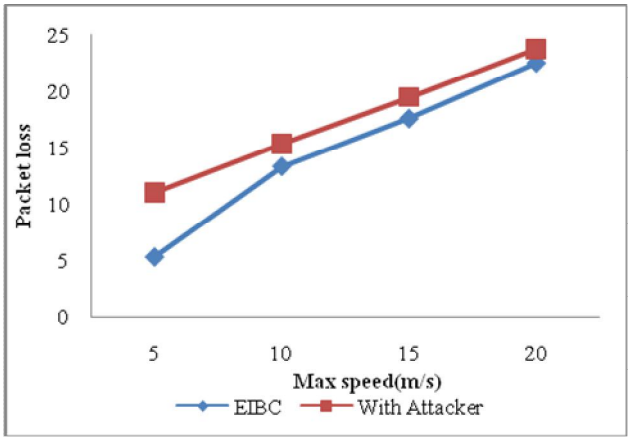


Figure 5: Max speed vs. Packet loss

From the graph, the x-axis is taken as the maximum speed which is measured in terms of metre per second. The y-axis is taken as packet loss which is measured in terms of numbers. When the maximum speed increases the packet loss is also increased. But when the attacker is detected and before prevented, the packet loss is increased. Then compare it with after prevention, the security mechanism EIBC which is introduced in AODV protocol produces a reduced packet loss and then achieved the recovered performance.

6.CONCLUSION

The security mechanism called Enhanced Identity Based Cryptography is constructed in mobile ad hoc network environment. The node id is assigned for each and every node in a MANET. Then the public and private key is generated with the use of node's id and secret value. The encryption and signature verification is done with the use of public and private keys. The brute force attack is detected and prevented with the use of encryption and verification process in the network environment. The performance is analyzed when there is no security mechanism and when there is security mechanism.

REFERENCES

[1] Aarti and Dr.S.S Tyagi, "Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), , vol. 3, no. 5, pp. 252-257, 2013.

[2] Priyanka Goyal,Vinti parmar and Rahul rishi, "MANET: Vulnerabilities, Challenges, Attacks, Application",International Journalof Computational Engineering and Management (IJCEM), vol.11,pp.32-37, Jan 2011.

[3] H.Yang,H. Luo,F.Ye,S.Lu and L.Zhang,"Security in mobile ad hoc networks:challenges and solutions,"IEEE Wirel. Commun.,vol. 11,no. 1, pp. 38–47, 2004 .

[4] K.Sangeetha, "Secure Data Transmission in MANETS Using ELIPTIC Curve Cryptography" International Journal of Innovative Research in Computer and Communication Engineering,vol. 2,no. 1, pp. 2557-2562, Mar 2014.

[5] Shushan Zhao, Akshai Aggarwal et al., "A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Networks" IEEE communications surveys & tutorials, vol. 14,no.2, pp.380-400, 2012.

[6] Abdul Manaf, Babak Emami et al., "Enhancing Security for Mobile Ad hoc Networks by Using Identity Based Cryptography" International Journal of Computer and Communication Engineering,vol. 3,no.1, pp.41-45, 2014.

[7] Craig Gentry and Alice Silverberg, "Hierarchical ID-Based Cryptography" ad hoc networks,vol.2501, pp.548-566, 2002.

[8] A.Kahate and V.Chandure et al., "Improving authentication mechanism for using extended public key cryptography in mobile adhoc network" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 2,no.4, pp.1322-1329, 2013.

[9] R. Vedhavarshini and T. Anand, "Efficient Data Packet Transmission in MANET Using Enhanced Hybrid Cryptographic Technique" International Journal of Computer Science and Information Technologies, vol. 5,no.3, pp.3309-3311, 2014.

[10] Anil Kapil and Sanjeev Rana, "Identity-Based Key Management in MANETs using Public Key Cryptography" International Journal of Security (IJS), vol. 3,no.1, pp.1-8, 2011.

[11] Vinayak & Nahala, "Avoiding Brute Force attack in MANET using Honey Encryption" International Journal of Science and Research (IJSR),vol. 4,no.3, pp.83-85, 2015.
[12] Vanesa Daza, Javier Herranz et al., "Cryptographic techniques for mobile ad-hoc networks" Computer Networks 51, pp.4938-4950, 2007.
[13] R. K. Sharma, Neeraj Kishore and Parijat Das, "Secure and efficient application of MANET using Identity Based cryptography combined with Visual cryptography technique" International Journal Of Engineering And Computer Science , vol. 3,no.2, pp.3933-3937,2014.
[14] Shane Balfe, Kent D. Boklan, Zev Klagsbrun and Kenneth G. Paterson, "Key Refreshing in Identity-based Cryptography and its Application in MANETS" Military Communications Conference,pp.1-8,2007.
[15] Hasaen Nicanfar and Victor C.M Leung, "EIBC : Enhanced Identity- Based Cryptography, a conceptual design" IEEE Systems conference, pp.1-7,2012.

Authors

Ms.P.Subbulakshmi, B.Tech (IT).,M.E.,is currently Working as a Assistant. Professor in Department of Information Technology, National Engineering College, Kovilpatti,Tamilnadu.She has around Five years of teaching experience. She has published several papers in lot of Journals, Conferences. Her modest areas of interest include MANETs, cryptography& Wireless Networks & security.
Email:subbu.psk@gmail.com

Mr.S.Vimal,B.Tech (IT)., M.B.A.,M.E.,MISTE.**,** is currently Working as a Assistant. Professor in Department of Information Technology, National Engineering College, Kovilpatti,Tamilnadu.He has around Nine years of teaching experience. He is a CISCO (CCNA) certified professional and being members in academic societies like ISTE, IEEE, and National Book Trust. He has published several papers in lot of Journals, Conferences. His modest areas of interest include Cloud Computing, Cognitive networks,MANETs,cryptography, WirelessNetworks.

Email:vimal28.05.1984@gmail.com