ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

Prevention of Collaborative Attacks using Elliptic Curve Diffie-Hellman in MANET

Shabnam. S[1], **Ramesh. T**[2]

[1] PG Scholar (CSE), RMK Engineering College, Kavaraipettai, Tiruvallur District, Tamil Nadu, India

[2] Assistant Professor (CSE), RMK Engineering College, Kavaraipettai, Tiruvallur District, Tamil Nadu, India

ABSTRACT : In past few decades, the migration of communication occurs from wired networks to wireless networks because of its mobility and scalability and MANET (Mobile Ad hoc Network) is a unique and significant application in recent years which does not necessitates any pre-existing network infrastructure. MANETs are Multi hop networks comprises of thousands of mobile nodes which are autonomous and can move along the network that forms a temporary dynamic network. The fundamental necessity of mobile network is the cooperation of mobile nodes to make communication among them that causes serious security problems. For example consider a malicious nodes present in the network which may disrupt the routing process. For that Ad hoc On demand Distance Vector (AODV) with Elliptic Curve Diffie-Hellman (ECDH) technique is proposed to overcome such difficulty. The proposed technique detects malicious nodes to prevent the network. ECDH shares secret key between source node and destination node by employing its public and private key. Through this it ensures security of the network. Finally, the proposed work is compared to the existing or previous works and the experimental results are shown in graph.

KEYWORDS: MANETs, ECDH, Ad hoc On demand Distance Vector (AODV), collaborative black-hole attacks and malicious node.

I.INTRODUCTION

Generally, wireless networks possess flexible mobility and scalability for several communications. So, they are always chosen for various applications from the beginning of their innovation. These wireless networks are considered as an improved technology which has minimum cost for communication compared to wired networks and they gained more popularity in the field of research, industrial and academic. MANET (Mobile As hoc Network) is a significant concept of wireless networks which comprises of thousands of nodes that are mobile as well as autonomous and they do not requires any existing network infrastructure.

The autonomous nodes can freely and randomly move within the network which can create temporary dynamic network and these networks can change their topology frequently. [1]. Each and every activity like node discovery and data delivery is performed by the autonomous nodes separately or conjointly. The nodes of MANETs are fitted with both wireless transmitter as well as receiver which can communicate with each other through the wireless links in a direct or indirect manner and now-a-days industrial applications like remote access and control through the wireless links getting more fame.

The MANET structure depends on their applications that may vary from modest, static network which is extremely power-consumed to large scale dynamic mobile networks. MANETs are classified into two types such as open and closed in which the closed mobile networks are commonly used for emergency applications such as military and rescue services etc and their nodes get together towards a general destination. In an open mobile network, various mobile nodes work with several goals but they share common resources to assure worldwide connectivity. [2, 3].

Moreover, the nodes of mobile networks can able to provide data communication among various users with constant mobility and after data communication it keeps their mobility as same level. This is the main advantage of wireless network over wired network. The communication is restricted to the nodes which are in various communication ranges and the

DOI: 10.15680/IJIRCCE.2015. 0310089

mobile nodes can solve such problem by permitting intermediate nodes to execute data transmission. This is done by splitting MANETs into two cases of networks such as single-hop and multi-hop. If the nodes are in the same communication range and can communicate directly with each other is considered as a single-hop network and in multi hop networks the nodes are in different communication range in which intermediate nodes are preferred for communication in an indirect manner. [4].

Minimum constellation and frequent deployment create mobile network ready to be employed in emergency considerations where a substructure is not available or impracticable to establish in the following cases such as natural or human- caused tragedies, military battles, and medical exigency conditions. Because of the above unique features, MANETs are widely employed in various industrial applications. However, believing the concept that MANET is famous within vital mission features, security of network is of much more important. Regrettably, the characteristics like open medium and remote dispersion of mobile networks causes it vulnerable to various attacks and the distributed architecture and frequently varying topologies, a conventional centralized monitoring approaches is no more executable in MANETs. [5].

Section 2, overview the operations of existing protocols and section 3 explains ECDH in Mobile Ad hoc Networks. In Section 4, talk about the proposed technique and section 5 reviews the performance analysis. Section 6, shows the experimental results. Finally, Section 7 concludes the paper.

II.RELATED WORK

There are several proposals based on ECDH that advertise to guarantee security in Ad-hoc networks which are discussed in this section.

According to [6]: The Elliptic Curve Diffie-Hellman (ECDH) key agreement scheme is a variant of the Diffie- Hellman key agreement protocol. The Elliptic Curve Digital Signature Algorithm (ECDSA) is a variant of the Digital Signature Algorithm (DSA). The Elliptic Curve Integrated Encryption Scheme (ECIES) is a public-key encryption scheme which provides semantic security against an adversary who is allowed to use chosen plaintext and chosen-cipher text attacks, also known as the Elliptic Curve Augmented Encryption Scheme (ECAES) or simply the Elliptic Curve Encryption Scheme.

Other extensions as shown in [22] are: The Group Elliptic Curve Diffie-Hellman (GECDH) protocol which is an extension of GDH based on ECDLP, and Tree-based Group Elliptic Curve Diffie-Hellman (TGECDH) which is a variant of TGDH based on ECDLP.

The organization of the network nodes is one of the features that take into account the proposals based on ECC due to dynamic network topology. For example [7] presents an organization of the nodes through a Region-Based Group, where a group of nodes in a region, which in turn is divided into sub-groups that are responsible for keeping your keys using GECDH Protocol and links with other subgroups in a tree structure using TGECDH protocol with nodes which are assigned tasks of communication management. A similar organization is found in [8] based on networks Near Term Digital Radio (NTDR) presents an organization Cluster-based where all mobile nodes are divided into different clusters controlled by cluster heads and with two Classes of communication intra-cluster and inter-cluster using ECC.

When implementing ECC in MANET, the Related Works focus on the type of Key Establishment Process to use. Some proposals use Key Management Protocols as in [10] with Cluster-based organization, or [9] with Threshold organization. Another proposals applying ECC in MANET with Key Management are: [11, 12]. Some proposals use Key Agreement Protocols as [14] that seeks resist the offline password guessing attack, others simply apply ECDH in its Key Agreement Protocol as [13]. Other proposals applying ECC in MANET with Key Agreement are [7] and [18].

Some proposals study the application of software libraries to implement ECC on MANET as [6] and [17]. In [16] is presented a fuzzy controller for a dynamic window sizing to optimize the calculation of an ECC scalar multiplication and evaluate their performance in MANET. In [15] is sought through the code development over some microcontrollers the optimization faster implementation of an ECC in MANET. In [21] is compared the application of ECC versus RSA in MANET in order to observe their strengths and in [25] shows how some ECC implementations have some limitations on MANET performance.

III.ECDH in MANET

There are many reasons why there have been introduced the concept of ECDH in MANET. According to [19] and [20], Compared to traditional cryptosystems like RSA, ECDH offers equivalent security with smaller key sizes, faster computation, lower power consumption, as well as memory and bandwidth savings. This is especially useful for mobile devices which are typically limited in terms of their CPU, power and network connectivity. In [21], it is shown how the energy cost for RSA is greater than that of an ECDSA (a Signature Algorithm of ECDH) showing better performance.

However, in [22] although it is recognized that attraction of ECDH is that it appears to offer equal security for a far smaller key size, thereby reducing processing overhead, also is showed that: the methods for computing general elliptic curve discrete logarithms are much less efficient than those for factoring or computing conventional discrete logarithms and it indicates that more computation time is required for ECDH and considers that the overall performance of ECDLP-based applications needs to be evaluated. However, compared to many other conventional cryptosystems, ECDH is a very good alternative to the characteristics of a MANET.

IV PROPOSED TECHNIQUE

4.1. Elliptic Curve Diffie-Hellman (ECDH)

An Elliptic Curve Diffie-Hellman (ECDH) [23] is a public key system based on Diffie-Hellman methods and Digital Signature Algorithm (DSA), but instead of using whole numbers as the symbols of the alphabet of the message to digitally sign or encrypt, uses points in a mathematical object called Elliptic Curve.

An elliptic curve is a plane curve defined by a cubic equation (third degree) as:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5 \quad (1)$$

4.2. Key Establishment Process

The process by which two or more entities (in our case Ad-Hoc nodes) establish a shared secret key (session key) in order to be used to achieve some cryptographic goals, such as confidentiality or data integrity is called: Key Establishment Process [24].

We can classify the Key Establishment Process by its distribution, or by the prior information that each entity has before starting the process:

A. By its distribution: The key distribution problem in MANET is the problem of how to set up secret keys between communicating nodes [25]. There are two possible modes of distribution: Key Transport and Key Agreement.

- Key Transport Protocols: A key is generated by one entity sometimes called CA (Certificate Authority) and then is transmitted through a secure channel to a second entity [24]; this mode of distribution is also known as Key Management.

- Key Agreement Protocols: Also known as Key Exchange Protocols both parties perform a negotiation process in order to contribute information to generate and exchange a secret key.

B. By the prior information: There are two possible modes of Key Establishment: Symmetric and Asymmetric protocols.

- Symmetric Protocols: The two entities have from the beginning of the process common secret information for the establishment of the key.

- Asymmetric Protocols: The two entities involved only share public information that has been authenticated previously.

4.3. Key Sharing Mechanism (ECDH)

ECDH ensures secrete key between two parties by using their public data and private data. Third party does not know the private data by using any public data of node. Before establishing the shared key both parties should agree on domain parameters. Node can generate public key as Q=s*G. let (si, Qi) be the pair of the private key-public key of node Ni and (sj,Qj) be the pair of private key-public key of node Nj. the following steps explains algorithm for key establishing between two parties.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

1. The end node N_i computes $K = (xK, yK) = s_i * Q_i$
2. The end node N_j computes $L = (xL, yL) = s_j * Q_j$
3. Since, $s_i * Q_i = s_i * s_j * G = s_j * s_i * G = s_j * Q_j$ Therefore K=L and hence xK=xL.
4. Hence the shared secret is xK.

V.PERFORMANCE ANALYSIS

In this section, the performance of the proposed AODV based approach and existing Dynamic Static Routing (DSR) based approach are compared. The metrics used for the performance evaluation of the proposed AODV based approach and existing DSR based approach are given in Table 2.

5.1. Security analysis

The expedited triple key broadcast authentication scheme is compared with various existing broadcast authentication and security schemes in WSN. The network architecture composes of 300 nodes in a simulated area of 1000 * 1000 m. The nodal velocity is varied from 5 to 30 m/s. They are analyzed in terms of communication overhead, energy consumption and time taken for various cryptographic processes, such as key setup, encryption, decryption, key extraction, signature establishment, and signature verification. The detection rate of attacks in the WSN is analyzed in terms of the detection accuracy and its false positive rate (FPR). The various techniques are also compared in terms of capability of detecting various attacks, memory consumption, resiliency, and the probability of hash value being compromised versus the number of compromised nodes.

Simulation Parameters	Values
Network interface type	Phy/wirelessPhy
MAC type	MAC/802_11
Interface queue type	Queue/DropTail/PriQueue
Link layer type	LL
Antenna model	Antenna/OmniAntenna
Max packet in ifq	50
Number of mobile nodes	100
Routing protocol	AODV
X dimension of topography	500
Y dimension of topography	500
Time of simulation end	100.0
Energy setup	Energy

Table 2: Parameter Comparison

DOI: 10.15680/IJIRCCE.2015. 0310089

VI.EXPERIMENTAL RESULTS

6.1. End to end delay

End-to-End delay is the time taken for a packet to be transmitted from the source to the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Figure.2 shows the comparison graph depicting the end-to-end delay of the existing DSR and proposed AODV based approaches. The End-to-End delay of the proposed AODV based approach is found to be lower than existing DSR based approach.

6.2. Energy consumption

Energy consumption is defined as the amount of energy required for transferring packet to the next nodes. Figure.3 shows the comparison graph of the node energy of the proposed AODV based approach and DSR based approach. The energy of the proposed approach is lower than the existing approach. Hence, the proposed approach achieves high energy efficiency.

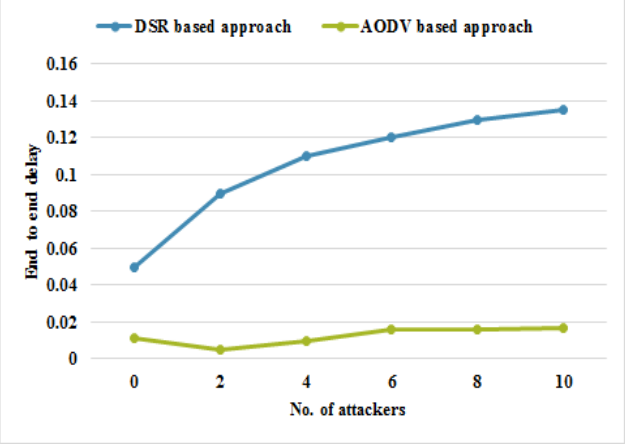

Figure 3: Delay time Vs No. of attackers

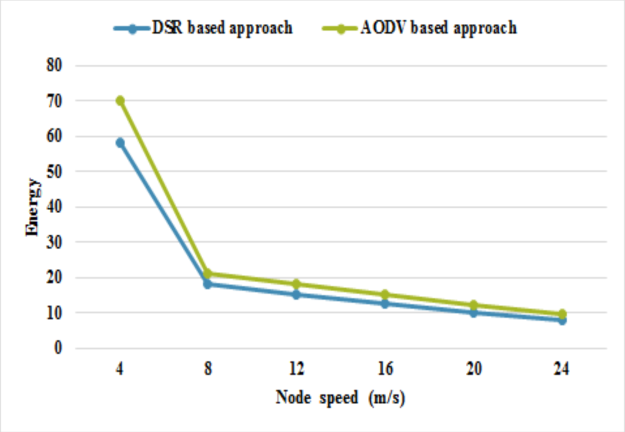

Figure 4: Node energy Vs node speed

6.3. Routing failure

Routing failure is defined as the total number of packets lost during data transfer. Figure 4 shows the comparison graph of the existing DSR based approach and AODV based approach. From the comparison graph, it is clearly observed that the throughput of the proposed approach is higher than the existing technique.

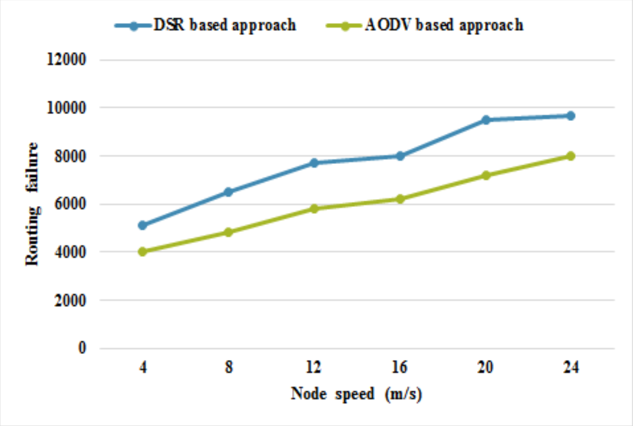

Figure 5: Routing failure Vs node speed

6.4. Routing Overhead

The ratio of total number of the control packets generated in the network to the total number of the data packets received. Figure.5 shows the comparison graph depicting the routing overhead of the existing DSR and proposed AODV based approaches. The proposed approach achieves low routing overhead than the existing approach.

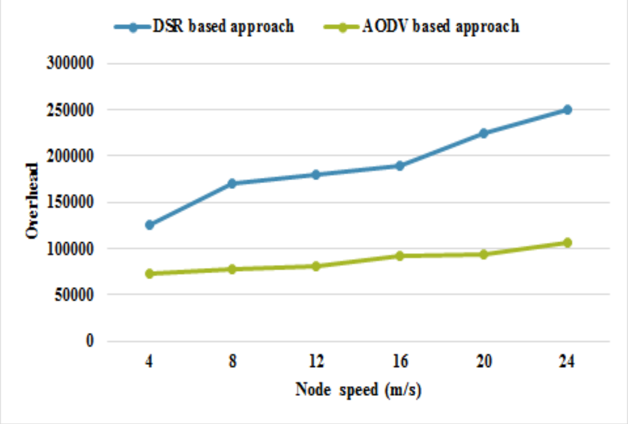

Figure 6: Overhead Vs Node speed

6.5. Packet Delivery ratio (PDR)

Delivery ratio can be defined as the ratio between the number of messages delivered/ received and the number of messages sent.

DOI: 10.15680/IJIRCCE.2015. 0310089

$$PDR = \frac{Number\ of\ packets\ received}{Number\ of\ packets\ transmitted} * 100$$

The PDR is the ratio of the number of delivered data packets to the destination. Figure.6 shows the graph illustrating the packet delivery ratio of the proposed AODV based approach and existing DSR based approach. The PDR of the proposed approach is higher than the existing approach.

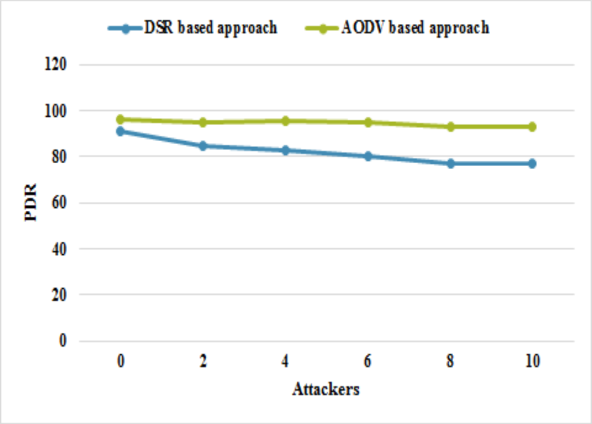

Figure 7: PDR Vs attackers

6.6. Throughput

Throughput is the average rate of successful data delivery over the channel and it is measured in data packets per time slot. Figure.7 shows the comparison graph of the throughput of the existing DSR based approach and AODV based approach. From the comparison graph, it is clearly observed that the throughput of the proposed approach is higher than the existing technique.

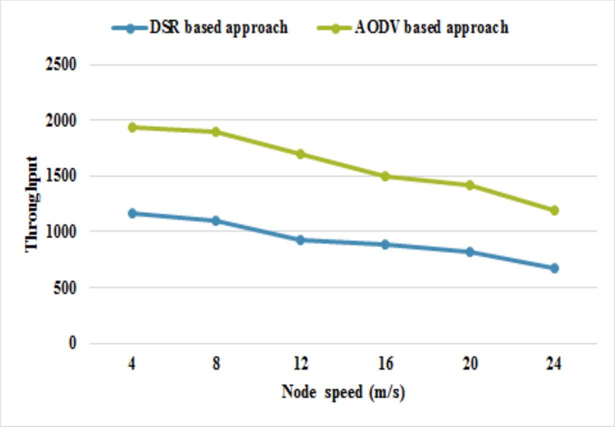

Figure 8: Throughput Vs node speed

DOI: 10.15680/IJIRCCE.2015. 0310089

Hence, it is concluded that the proposed AODV based approach achieves better performance than the existing DSR based approach.

VII.CONCLUSION

Mobile Ad hoc Networks (MANETs) are prone to various attacks because of their hostile environment. The security of a MANET is critical especially in military communications. The expedited ECDH (Elliptic Curve Diffie-Hellman) key agreement scheme, and ECDSA (Elliptic Curve Digital Signature Algorithm). The signature verification process is accelerated by releasing few intermediate computation results in the MANET by the mobile nodes. It performs better compared to other security schemes, in terms of accuracy, detection of attacks, resiliency, memory consumption, nodal detection, and average of total transmission energy consumed per node.

REFERENCES

[1] H. Miranda and L. Rodrigues, ―Preventing Selfishness in Open Mobile Ad Hoc Networks,‖ Proc. Seventh CaberNet Radicals Workshop, Oct. 2002.
[2] Y. Kim, "Remote sensing and control of an irrigation system using a distributed wireless sensor network," IEEE Trans. Instrum.Meas., vol. 57, no. 7, pp. 1379–1387, Jul. 2008.
[3] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocol—A review," J. Comput. Sci., vol. 3, no. 8, pp. 574–582, 2007.
[4] B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.
[5] A. Tabesh and L. G. Frechette, "A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micropower generator," IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 840–849, Mar. 2010.
[6] An Liu; Peng Ning; , "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks," Information Processing in Sensor Networks, 2008. IPSN '08. International Conference on , vol., no., pp.245-256, 22-24 April 2008.
[7] Kumar, K.; Begum, J.N.; Sumathy, V.; , "A Novel Approach towards Cost Effective Region Agreement Protocol for Ad Hoc Networks," Intelligence, Communication Systems and Networks, 2009. CICSYN '09. First International Conference on pp.470-475, 23-25 July 2009.
[8] Jing-feng Li; Ya-juan Zhang; Yue-fei Zhu; , "A secure elliptic curve communication scheme for the cluster ad hoc networks," Wireless, Mobile and Multimedia Networks, 2006 IET International Conference on pp.1-4, 6-9 Nov. 2006.
[9] Dahshan, Hisham; Irvine, James; , "A Threshold Key Management Scheme for Mobile Ad Hoc Networks Using Elliptic Curve Dlog-Based Cryptosystem Networks and Services Research Conference (CNSR), 2010 Eighth Annual , vol., no., pp.130-137, 11
[10] Xiaojiang Du; Guizani, M.; Yang Xiao; Hsiao "A routing-driven Elliptic Curve Cryptography based key management scheme for Heterogeneous Sensor Networks," Wireless Communications, IEEE Transactions on no.3, pp.1223-1229, March 2009.
[11] Huaqun Wang; Shuping Zhao; Guoxing Jiang; , "Key Management Based on Elliptic Curve Paillier Scheme in Ad Hoc Networks," Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007. Eighth ACIS International Conference on , vol.1, no., pp.116-119, July 30 2007-Aug. 1 2007.
[12] Dahshan, H.; Irvine, J.; , "An Elliptic Curve Distributed Key Management for Mobile Ad Hoc Networks," Vehicular Technology Conference (VTC 2010-Spring), 2010 IEEE 71st , vol., no., pp.1-5, 16-19 May 2010.
[13] Du Congwei; Li Rongsen; Dou Wenhua; , "An efficient key agreement protocol in cluster-based MANETs," Computer Application and System Modeling (ICCASM), 2010 International Conference on , vol.10, no., pp.V10-627-V10- 630, 22-24 Oct. 2010.
[14] Chin-Chen Chang; Shih-Chang Chang; , "An Improved Authentication Key Agreement Protocol Based on Elliptic Curve for Wireless Mobile Networks," Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP '08 International Conference on , vol., no., pp.1375-1378, 15-17 Aug. 2008.
[15] B. Erik-Oliver, M. Zitterbart, "Efficient Implementation of Elliptic Curve Cryptography for Wireless Sensor Networks", Telematics Technical ReportsTM-2005-1, 2005
[16] Xu Huang; Sharma, D.; , "Fuzzy controller for a dynamic window in elliptic curve cryptography wireless networks for scalar multiplication," Communications (APCC), 2010 16th Asia-Pacific Conference on , vol., no., pp.458-463, Oct. 31 2010-Nov. 3 2010.
[17] Wang Wei-hong; Lin Yu-bing; Chen Tie-ming; , "The study and application of elliptic curve cryptography library on wireless sensor network," Communication Technology, 2008. ICCT 2008. 11th IEEE International Conference on , vol., no., pp.785-788, 10-12 Nov. 2008.
[18] Zhang Li-Ping; Cui Guo-Hua; Yu Zhi-Gang; , "An Efficient Group Key Agreement Protocol for Ad Hoc Networks," Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on , vol., no., pp.1-5, 12-14 Oct. 2008.
[19] V. Katiyar, K. Dutta, S. Gupta; "A Survey on Elliptic Curve Cryptography for Pervasive Computing Environment." International Journal of Computer Applications 11(10):41– 46, December 2010.
[20] Xu Huang; Shah, P.G.; Sharma, D.; , "Protecting from Attacking the Man-in-Middle in Wireless Sensor Networks with Elliptic Curve Cryptography Key Exchange," Network and System Security (NSS), 2010 4th International Conference on , vol., no., pp.588-593, 1-3 Sept. 2010.
[21] Jia Xiangyu; Wang Chao; , "The application of elliptic curve cryptosystem in wireless communication," Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications, 2005. MAPE 2005. IEEE International Symposium on , vol.2, no., pp. 1602- 1605 Vol. 2, 8-12 Aug. 2005.

[22] Yong Wang; Ramamurthy, B.; Xukai Zou; , "The Performance of Elliptic Curve Based Group Diffie-Hellman Protocols for Secure Group Communication over Ad Hoc Networks," Communications, 2006. ICC '06. IEEE International Conference on , vol.5, no., pp.2243-2248, June 2006.

[23] N. Koblitz, “Elliptic curve cryptosystems,” Mathematics of Computation,vol. 48, no.177, pp.203-209, Jan 1987.

[24] S. Blake-Wilson, A. Menezes, "Unknown Key-Share Attacks on the Station-to-Station (STS) Protocol.", Public Key Cryptography, Second International Workshop on Practice and Theory in Public Key Cryptography, PKC '99, Kamakura, Japan, Proceedings, pages: 154-170, 1999.

[25] P. Szczechowiak, L.B. Oliveira, M. Scott, M. Collier, and R. Dahab, "NanoECC: Testing the Limits of Elliptic Curve Cryptography in Sensor Networks", in Proc. EWSN, 2008, pp.305-320.