Journal of Theoretical and Applied Information Technology
15th March 2017. Vol.95. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

IDENTITY BASED CRYPTOGRAPHY FOR MOBILE AD HOC NETWORKS

V.LAKSHMAN NARAYANA[1], Dr.C.R.BHARATHI[2]

[1]Research Scholar, Department of CSE, Veltech University, Avadi, Chennai
Asst.Professor, Vignan Nirula Institute of Technology & Science for Women, Guntur

[2]Assoc.Prof, Department of ECE, Veltech University, Avadi, Chennai, Tamil Nadu, India

Email: [1]lakshmanv58@gmail.com, [2]crbharathi@veltechuniv.edu.in

ABSTRACT

MANETs (Mobile Ad Hoc Networks) are facing the common problems in providing security in all aspects. Their natural characteristics make them vulnerable to passive and active attacks, in which misbehaving nodes can eavesdrop or delete packets, modify packet contents. The Identity-based cryptography system to MANET mainly concentrates on deal out the responsibility of consistent ability among the multiple nodes in a network. Cryptographic technique which uses public key is the mechanism considered in this regard. Secret sharing mechanism is adopted by many existing systems which involves secret sharing of keys to a trusted node among nodes in a network which increases security level. Here we propose threshold cryptography which makes the authority more robust against network disasters and harder to negotiation. Identity-based cryptography, where any identity may assist as a public key, makes certificates and certificate distribution superfluous. The authority distributing private keys corresponding to identities is called a Private Key Generator (PKG). The proposed method deliberates distributing a PKG towards the nodes in the MANET. It shows the security properties of the base IBC systems are preserved when this distributed PKG is used instead of the original.

Keywords: *Cryptography, key generation, public key, MANET, private key generation (PKG)*

1. INTRODUCTION

A mobile ad hoc network (MANET) is a group of nodes dynamically grouped together to form a network and does not rely on fixed substructure, their networking setting is on the crest of ad hoc network group. In addition, it is continuously self-configuring, unguided network of mobile devices connected as a group .Each node should be ready to onward data to other destination nodes at any moment. Every authenticated node has a link with the remaining group, supposed to be neighboring nodes in the ad hoc network. The Number of nodes involved in the ad hoc network is not an essential constraint to consider. Here nodes are molded and fragmented with mobility and has partial battery control. Securing MANETs and WSNs is a important task which can be achieved by considering the factors for: vibrant topology structure, considering required resources, infrastructure-less and restricted substantial protection. WSNs are developed with more nodes when compared to MANETs, and sensor nodes in WSNs are more resource controlled in terms of authority, calculating capabilities, and memory requirements, WSNs security designs are more specific for those areas. A great research has been conducted on Secure routing, management of keys, and confidence in MANETs and WSNs; much of these issues is associated with cryptography mechanisms , strong validation, valid approval, encryption, and decryption (Chen & Wu, 2010). The essential security necessities for MANETs contain (Abusalah *et al*., 2008): Data privacy that keeps sensitive data secret to outsiders of a network, Data reliability that avoids data from being disturbed, Data sorting that keeps data in the correct arrangement, Data accessibility where requested data is made available, Identity certification of sensitive data that cross-checks whether the data or request came from a specific node and valid sender or not, and Non-repudiation that indicates a node cannot refuse sending a

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

message to the required nodes. For MANETs, security mechanisms which are strong and are adopted by guided networks are not always adopted. Attacks in wired networks that can be easily detected also became a big security challenge to MANETs. Examples contain, but are not limited to, uniqueness/address spoofing, data tampering and forgery, data repeat, changing routing information, etc (Zhao *et al*., 2012) Secure multitransmission (where a single data packet can be transmitted from a sender and transmitted to a group of receivers), secure direction-finding, privacy-aware routing, and key organization. Key organization is a major primary security issue because it is a central part of any secure communication are some of the complex problems faced by MANETs. The responsibilities of the key organization include generating the keys and distributing them securely and maintaning of keys.Maintenance of keys includes the actions for storing of keys securely , updating of keys frquently, and key revocation. For this purpose here we propose Threshold cryptography is an art of dividing a secret key for increasing security levels. Authenticating a user involves high security than non- threshold cryptographic schemes.

2. PROBLEM IDENTIFICATION

In MANETs applying cryptography mechanisms mainly concentrates on how divide up the responsibility of the trusted authority among the nodes in the network. In guided networks attacks can be easily and proficiently identified and prevented but the same thing a highly challenging task in MANETs. Examples include, but are not limited to, distinctiveness/address spoofing, data tampering and forgery, data repeat, changing routing information, etc. When this method is contrasted with guided networks, the following characteristics of MANETs make it problematical to achieve best security requirements:

- Maintain network substructure and online supervision is not performed.
- Network structure, its topology and membership dynamics of a node
- The possible insider attacks.

Therefore, most proposals consider some secret sharing techniques to protect mobile ad-hoc environments to distribute the key to a trusted entity. Here we propose Threshold cryptography to enhance the security to apply the relatively frequent key update technique.

3. RELATED WORK

Sumalatha and Sathyanarayana (2015) projected a technique for "Enhanced Identity-based cryptography towards multicast group key management" which considers PKI in distributed environments. IBC is intended to depend on an external member (trusted third party) for generating private keys using Private Key Generator (PKG). Before performing these operations, PKG is thought to produce a public key and private key pair. The proposed method is much suitable for real-world applications that are related with unguided transmissions providing good level of security and telecommunications which is distributed in nature. Such systems can influence scalability through the proposed IBC mechanism.

Jathe and Dhamdhere (2015) propose a Hybrid Cryptography with RSA Approach. Here the RSA stands for the name of the three researchers who designed it, Ron Rivest, Adi Shamir, and Leonard Adleman. Two major prime numbers are considered and their factorization is utilized as a part of RSA. The public key is considered for encrypting the data and for decrypting the data the key used is private. The source node is used to deliver packets to multiple destination nodes. Therefore, the path which is activated can be anyone. When a packet is sent from the source node to the next node then back acknowledgment is sent to the source node, which is also called as activation node. Acknowledgment is directly sent to the source node when provided packet is delivered from next node to destination node. At the same moment, the text, data, the packet which is encrypted with a digital signature at the source node, is decrypted at original message, i.e., text, data, packet at destination end.

Sharma *et al*. (2014) propose Visual Cryptographic technique, due to its simplicity and efficiency makes it the appropriate choice for sending / receiving images and finds use in transmitting encrypted images to and fro base station from border military forces. In its place of using only private key generators, both public - private key pairs are adopted to make the system more secure. Visual Cryptography Sharing Case with Two Shares, is a superior case of (2, N) visual cryptography case where N=2 and thus infers that the original image is divided into two shares, and to decrypt the information controlled in the original image these shares are required at destination node. Stacking the two shares into some transparency discloses information about the original image

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

while no information can be found from the separate shares.

Zamani and Zubair (2014) propose a cryptographic keying algorithm, the plan of this technique is providing secure methods for handling sensitive data. Key supervision contains keys for generation which are used for encryption and decryption, distribution and maintenance which involves sharing of keys among nodes in network and to store those keys in key pools. Maintenance of generated keys involves in updating of keys at regular time intervals,etc.

Honarbakhsh *et al*. (2014) propose IBC-t method key management for MANET. IBC-t is a certificates solution which allows public and private keys of mobile nodes proceed from a combination of their known ID and some other factors while is simple and unique without complex computationally. The concept of IBC-t method is a novel method of applying ID-Based public/private key which not only guarantees high-level authentication of mobile nodes but also facilitates efficient key generates which leads to resilience against node The major findings of this research improves authenticity and confidentiality through the network by reducing the computational time and enhancing the authentication of mobile nodes.

Kirubani and Anbukodi (2014) propose a digital signature algorithm. In this method the security in MANETs are subjected to ensure confidentiality between nodes, authentication of a node which is intended to involve in data transmission, integrity in the network, availability of nodes which are authenticated, and non-repudiation of nodes during communication. To confirm the accuracy of these constraints Digital signature methods are used. This mechanism is ensured by the message which is send to the hash function, the hash function is then handled and it is send to the message digest, this message is used to check whether the message is valid or not. And then it sends to the signature function; it checks the signature is a private key or public key. To verify the signature by applying public key or private key by using generalized as an information string.

Kamboj and Goyal (2015) aimed to describe the management of generated keys techniques in MANET. key management can be divided into symmetric and asymmetric key management. Using a selected cryptographic key the encrypted messages are strongly protected to improve the security levels, which is the scenario of cluster communication called group key. Efficient technique for key management in MANET‟s can be developed using a hybrid key management which can be predicted in future.

Khatoon and Thakur (2015) aimed to present a distributed key management scheme, where certificate-less public key cryptography (CL-PKC) and threshold cryptography is employed as a group. This technique not only achieves enhanced security attributes for key management in MANET but also eliminates the need for certificate-based public key distribution and the key escrow problem efficiently.

However, Sumalatha and Sathyanarayanaa (2015) proposed a complex technique and have some limitations with traditional PKI. Jathe and Dhamdhere (2015) concentrate on preventing attacks, which come from the attacker in the network, which can be harmful to the system.

4. IDENTITY-BASED CRYPTOGRAPHY

Encryption keys derived from user identities are useful in avoiding trust problems which are generally faced in certificate-based public key infrastructures (PKIs). These systems generally involve some trusted authorities, called private key generators; to compute users' private key from their identity information. The idea was proposed first by Shamir (2000).Many practical identity-based signature schemes (Fiat & Shamir, 1986; Guillou & Quisquater, 1988) have been devised. we purposely hop over a lot of the detail within the following

In Balfe *et al*. (2007), Balfe *et al*. conceive of that in IBC infrastructures, entities from multiple TAs may well be gift inside a bigger coalition structure, with every Ta issuance cryptologic keys to entities in its own security domain supported the work of (Hoeper & Gong, 2006b; Carman, 2005; Khalili *et al*., 2003; Matt, 2004) they propose a light-weight, generic and broadly speaking applicable framework enabling the refreshing of privates keys in coalition-forming things. They signify their contribution is that the improvement upon the apparent approach of merely distributing new non-public keys by encrypting them mistreatment the previous public keys. The authors claim that their theme is secure and state that the framework is applicable to modify secure interoperation between entities with totally different trustworthy authorities in dynamic coalition's environments, and is especially well-suited to coalition forming in computation and bandwidth limited MANET's.

Li *et al*., (2007) contemplate cross-domain key agreement in multi-domain impromptu

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

networks. They propose a replacement IBC scheme supported multiple PKGs, that is additionally appropriate for multi-domain impromptu networks. They assume that there are two PKGs—P KG1 and P KG2 two domains, that share identical system parameters, however, have totally different master private keys during this scenario, the theme provides encryption/decryption, sign/verify functions between the two domains.

Cai *et al*., (2005) apply IBC to see collaboration in MANET's. They determine the matter of peer collaboration in impromptu networks, particularly once some peers are autonomous, selfish, or malicious in large-scale, heterogeneous networks. The payment-incited mechanism is Associate in Nursing approach for this drawback. However, most existing electronic payment schemes either trust online interactive authorities or are too significant for MANET's.

5. PROPOSED METHODOLOGY

The following are the steps involved in the proposed method:

5.1 Shared Key Generation

In mobile ad hoc networks, the IBC relies on a shared-key generation phase. In this, the network nodes never met develop a shared key, and based on this key, further secure communications become feasible. In this method, we developed two fundamentally different methods to achieve this goal. One of these methods is based on a key pool and uses several large pools of keys that are implemented in network nodes, and another one is shared key based on public system parameters.

5.2 Private Key Method

The mechanism that is used for identity-based public/private-key generation for each node, whether it is a PKG or not, is very important. The proposed method contains a number of continuous, non-overlapping key update phases. Each phase is associated with a binary string, called a phase identifier. In the initialization phase, a random seed, phase identifier, is preloaded to every node. After deployment, each node can determine phase identifiers. In the proposed method, each public/private key pair is both node-specific and phase-specific.

5.3 Generating New Master Key Share

Nodes in a mobile ad hoc network may leave the network /enter randomly; consequently, this may define that the number of PKGs in the network at any one time is less than a certain threshold value. So, a MANET should be accomplished setting up a new PKG. To become a PKG, a network node must satisfy the following conditions.

- The lifetime of the node must be greater than an adequate period of time.
- The node must well behave throughout its lifetime; that is, it must not be found to be on a blacklist.
- The node must have enough capabilities(communicational, computational, energy) to act as a private key generation.
- If a node happens the above-mentioned constraints, then it is thought to be a trusted and capable node.

5.4 Certificate Chaining Method

Certificate Generation initially two neighboring nodes authenticate each other through the exchange of certificate issued by offline Trusted Third Party (TTP). Verification of the certificate is done by using the TTP's public key. Once this verification is successful, each node issues its own certificate to its neighbors and certificates are stored in its repository with validity time for each certificate.

5.5 Algorithm

```
if (my id is between 0 and 20)
 {
   Execute malicious behavior
 }
 else
 {
   Process the routing packet correctly
 }
```

6.DESIGN GOALS

In proposed research, three novel methods are proposed to eliminate the interdependency cycle between secure routing and security services. One of these methods utilizes a key pool to construct secure routes for the distribution of cryptographic materials while the second one is based on the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

pairing-based key agreement. Also, the proposed methods use threshold cryptography for shared secret key and private key generation to remove the single point of failure and distribute cryptographic services among network nodes. These features guarantee high levels of availability and scalability for the proposed methods. The third one is certificate chaining method used to reduce the vulnerability.

7. KEY MANAGEMENT IN MANET

Key management is a basic part of any secure communication. Most cryptosystems rely on some underlying secure, robust, and efficient key management system. Secure network communications normally involve a key distribution procedure between communication parties, in which the key may be transmitted through insecure channels. A framework of trust relationships needs to be built for authentication of key ownership in the key distribution procedure. While some frameworks are based on a centralized trusted third party (TTP), others could be fully distributed. For example, a certification authority (CA) is the TTP in asymmetric cryptosystems, a key distribution center (KDC) is the TTP in the symmetric system, and in PGP, no TTP is assumed. According to recent literature, the centralized approach is regarded as inappropriate for MANETs because of the dynamic environment and the transient relationships among mobile nodes. Most researchers prefer the decentralized trust model for MANETs. Several decentralized solutions have been proposed in recent papers with different implementations, such as how the CA's responsibility is distributed to all nodes, or to a subset of nodes (Wu *et al*., 2008).

7.1 Schemes of key management

7.1.1 Asymmetric key management schemes

In the recent research paper they have proposed different types of key management schemes for the MANETs. It is found that most of them are only based upon the public-key cryptography. The main aim is to distribute the functionality of CA's to multiple nodes. Lidong Zhou and Haas (1999) aimed to represent secure key management scheme with the use of threshold cryptography and by employing (t, n) however, the system can allow up to t-1 negotiated servers. Luo *et al*. (2004, 2001) aimed to propose a local key management scheme through which all the node are considered as servers and the certificate for the service is performed by a neighboring threshold number of nodes. Yi *et al*. (2001) put forward a similar scheme. The difference is that their certificate service is distributed to a subset of nodes, which are physically more secure and powerful than the others. Wu *et al*. (2007) also introduced a scheme that is similar to Yi, in which server nodes form a mesh structure and a ticket scheme is used for efficiency. Capkun *et al*. (2003) considered a fully distributed scheme that is based on the same idea of PGP. Yi and Kravits (2004) provided a composite trust model. Their idea was to take advantage of the positive aspects of both the central and fully distributed trust models.

7.1.2 Symmetric key management schemes

There is a research article which is based upon the symmetric-key cryptography for the MANET securing. For example, some of the symmetric key management schemes are proposed based upon the sensor node which is assumed as incapable to perform costly asymmetric computation cryptography. Pairwise keys are again loaded in to a node which is based upon the random distribution of key which is set of a key that has been loaded again. Chan (2004) aimed to introduce distributed symmetric key distribution scheme for the MANET. The main idea is each node should be preloaded with the set of keys from a large key pool (Chan *et al*., 2003; Du *et al*., 2005). Key pattern satisfies the property with the subset of nodes that find one common key and the identified common key should not come under collision of certain other nodes to come outside the subset. Chan and Perrig (2005) aimed to determine the asymmetric key scheme agreement for the sensor node. The main theme of this approach is that each node shares an irreplaceable key along with set of nodes aligned horizontally and vertically. Hence, the pair of nodes can trust one intermediate node in order to establish the common key.

7.1.3 Group key management schemes

Group-orientation and collaborative application in MANETs are active in the upcoming research areas. The group key management is considered as one of the building block for the secured group communication. Yet, the key management has a large group of dynamic problem because of security and scalability (Rafaeli &

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Hutchison, 2003). For example, when a new member is being added each time or the old member is ejected from that group the password in the group key is changed in order to ensure forward and backward security.

8. RESULTS AND DISCUSSION

This section discusses in detail about the performance of MANET through end to end. The present scenario mainly aims to key generation and packet transfer among the nodes using the cryptographic algorithm. In this algorithm cipher, package information is transformed among the nodes.

Simulation strategies and principles adopts separated object model with the base of two languages tclNS2 and C++ that fulfill the simulation achievement of the specific protocols and the nodes for configuration and network simulation environment establishment respectively. The below Table 1 refers to the parameters used in the aided software like NAM in order to make further studies and the simulation process and for the analysis result. In the first stage we have set the configuration of nodes properties, topology and other properties of the MAC layer such as protocol type, address type, modulation type, simulation type, channel type, rx, tx, sleep power, transmission way and idle.

Table 1: Parameters Used In Aided Software

Parameters	Value
Protocol used	MANET
Application traffic	CBR
Packet size	512
Number of nodes	20
Pause time	10s
Maximum speed	0-20m/s
Simulation time	600s
Traffic rate	5 packets/sec

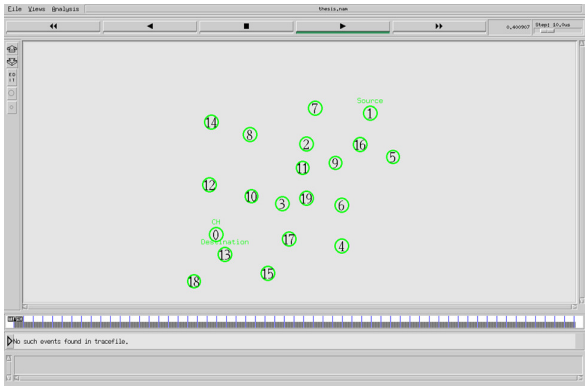

Fig.1 Creation Of Nodes

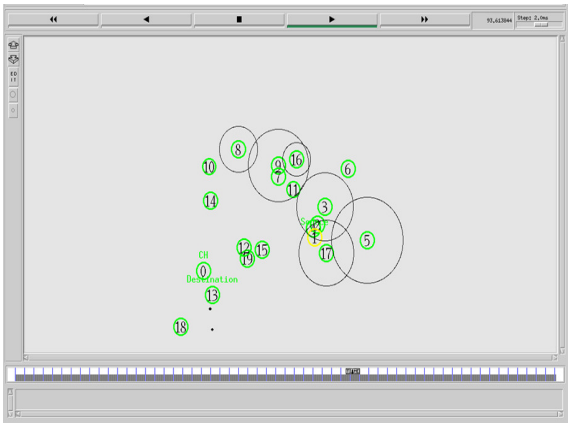

Fig.2 Distribution Of Keys Among Nodes

Key generation is used for generating the key using the output with a random bit generator. The key generation is derived from one key to another key and the particular key is derived using password and the agreement of key is performed based upon the two entities using an approved agreement key. The keys that are conquered is indirectly or directly present in the output of an approved random bit generator (RBG). Hence, the key are derived from the key transaction agreement that are derived from the another key with the use of key derivation function or derived from a password that are obtained in the storage application which is indirectly related to the RBG since the ancestor key or random value is directly formed from the output of RBG. The cryptographic keys are being generated by the cryptographic modules. For instance consider a cryptographic module is used to generate the key-generating module. The generated keys are then transformed using a more secured channels which associate the cryptographic algorithm.

9. CONCLUSION

MANET is used usually when a network need to work with the absence of TTP (trusted third party). This is one of the finest ways to achieve the property of third party by sharing the nodes. There is an essential tool that uses sharing secret

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

techniques. Conversely, there use of standard sharing of secretes key technique that makes use of dynamism which is very difficult to achieve. In the present paper, we have developed a key generation protocol for the IBC. In this IBC is a subclass that does not restrict the key cryptography. IBC is tending to remove the need for certification authority (CA) and public key certificates (PKCs). In this IBC for a user that is given is used as user's public key and private key which is depend upon the individuality of the user. In this IBC scheme the user is unrestricted with the designed function identity when the user's private key is being used by the trusted authority. In this IBC scheme the users are not restricted easily and they are easily designed function with the identity of the private key that is PKG. When comparing with the traditional PKI(public key infrastructure) the IBC is required in order to transmit and store the large volume of certificates and public key hence MANET is used.

REFERENCES:

[1] Abusalah, L., Khokhar, A. & Guizani, M. (2008). A survey of secure mobile Ad Hoc routing protocols. *IEEE Communications Surveys & Tutorials*. [Online]. 10 (4). pp. 78–93. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4738467.

[2] Balfe, S., Boklan, K.D., Klagsbrun, Z. & Paterson, K.G. (2007). Key Refreshing in Identity-Based Cryptography and its Applications in MANETs. In: *MILCOM 2007 - IEEE Military Communications Conference*. October 2007, IEEE, pp. 1–8.

[3] Cai, L., Pan, J., Shen, X. & Mark, J.W. (2005). *Peer Collaboration in Wireless Ad Hoc Networks*. In: pp. 840–852.

[4] Capkun, S., Buttyan, L. & Hubaux, J. (2003). Self-organized public-key management for mobile ad hoc networks. *IEEE Transactions on Mobile Computing*. [Online]. 2 (1). pp. 52–64. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1195151.

[5] Carman, D.W. (2005). New Directions in Sensor Network Key Management. *International Journal of Distributed Sensor Networks*. 1 (1). pp. 3–15.

[6] Chan, A.C.-F. (2004). Distributed symmetric key management for mobile ad hoc networks. In: *IEEE INFOCOM 2004*. [Online]. 2004, IEEE, pp. 2414–2424. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1354663.

[7] Chan, H. & Perrig, A. (2005). PIKE: peer intermediaries for key establishment in sensor networks. In: *Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies.* [Online]. 2005, IEEE, pp. 524–535. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1497920.

[8] Chan, H., Perrig, A. & Song, D. (2003). Random Key Predistribution Schemes for Sensor Networks. In: *Proceeding SP '03 Proceedings of the 2003 IEEE Symposium on Security and Privacy*. 2003, Washington, DC: IEEE Computer Society, pp. 1–197.

[9] Chen, J. & Wu, J. (2010). A Survey on Applied Cryptography in Secure Mobile Ad Hoc Networks and Wireless Sensor Networks. In: *Handbook of Research on Developments and Trends in Wireless Sensor Networks*. [Online]. Florida: IGI Global, pp. 262–289. Available from: http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-61520-701-5.ch012.

[10] Du, W., Deng, J., Han, Y.S., Varshney, P.K., Katz, J. & Khalili, A. (2005). A pairwise key predistribution scheme for wireless sensor networks. *ACM Transactions on Information and System Security*. [Online]. 8 (2). pp. 228–258. Available from: http://portal.acm.org/citation.cfm?doid=1065545.1065548.

[11] Elizabeth, E., Subasree, S. & Radha, S. (2014). Enhanced Security Key Management Scheme for MANETS. *WSEAS Transactions on Communications*. 13. pp. 15–25.

[12] Fiat, A. & Shamir, A. (1986). How To Prove Yourself: Practical Solutions to Identification and Signature Problems. In: *Advances in Cryptology — CRYPTO' 86*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 186–194.

[13] Guillou, L.C. & Quisquater, J.-J. (1988). A 'Paradoxical' Indentity-Based Signature Scheme Resulting from Zero-Knowledge. In: *Advances in Cryptology — CRYPTO' 88*. New York, NY: Springer New York, pp. 216–231.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[14] Hoeper, K. & Gong, G. (2006a). Bootstrapping Security in Mobile Ad Hoc Networks Using Identity-Based Schemes with Key Revocation. In: *5th International Conference*. 2006, Germany: Springer Berlin Heidelberg, pp. 224–237.

[15] Hoeper, K. & Gong, G. (2006b). *Key Revocation for Identity-Based Schemes in Mobile Ad Hoc Networks*. In: pp. 224–237.

[16] Honarbakhsh, S., Latif, L.B.A., Manaf, A. bt A. & Emami, B. (2014). Enhancing Security for Mobile Ad hoc Networks by Using Identity Based Cryptography. *International Journal of Computer and Communication Engineering*. [Online]. 3 (1). pp. 41–45. Available from: http://www.ijcce.org/index.php?m=content&c=index&a=show&catid=40&id=344.

[17] Jathe, S.S. & Dhamdhere, V. (2015). Hybrid Cryptography for Secure Superior Malicious Behavior Detection and Prevention System for MANET's. *International Journal of Innovative Research in Science, Engineering and Technology*. 4 (7). pp. 5673–5680.

[18] Kamboj, P. & Goyal, N. (2015). Survey of Various Keys Management Techniques in MANET. *International Journal of Emerging Research in Management &Technology*. 4 (6). pp. 176–178.

[19] Khalili, A., Katz, J. & Arbaugh, W.A. (2003). Toward secure key distribution in truly ad-hoc networks. In: *2003 Symposium on Applications and the Internet Workshops, 2003. Proceedings.* 2003, IEEE Comput. Soc, pp. 342–346.

[20] Khatoon, S. & Thakur, B.S. (2015). Certificate Less Key Management Scheme in Manet Using Threshold Cryptography. *International Journal of Network Security & Its Applications*. [Online]. 7 (2). pp. 55–59. Available from: http://www.airccse.org/journal/nsa/7215nsa04.pdf.

[21] Kirubani, K. & Anbukodi, S.P. (2014). A Secure Intrusion Detection System for Manets by using Cryptographic Algorithms. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*. 3 (3). pp. 7923–7931.

[22] Li, F., Hu, Y. & Zhang, C. (2007). An Identity-Based Signcryption Scheme for Multi-domain Ad Hoc Networks. In: *Applied Cryptography and Network Security*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 373–384.

[23] Lidong Zhou & Haas, Z.J. (1999). Securing ad hoc networks. *IEEE Network*. [Online]. 13 (6). pp. 24–30. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=806983.

[24] Luo, H., Kong, J., Zerfos, P., Lu, S. & Zhang, L. (2004). URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks. *IEEE/ACM Transactions on Networking*. [Online]. 12 (6). pp. 1049–1063. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1369293.

[25] Luo, H., Zerfos, P., Kong, J., Lu, S. & Zhang, L. (2001). Providing Robust and Ubiquitous Security Support for Mobile Ad-hoc Networks. In: *Proceeding of The 9th International Conference on Network Protocols*. 2001, Washington, DC: IEEE Computer Society, pp. 1–251.

[26] Matt, B.J. (2004). Toward hierarchical identity-based cryptography for tactical networks. In: *IEEE MILCOM 2004. Military Communications Conference, 2004.* 2004, IEEE, pp. 727–735.

[27] Rafaeli, S. & Hutchison, D. (2003). A survey of key management for secure group communication. *ACM Computing Surveys*. [Online]. 35 (3). pp. 309–329. Available from: http://portal.acm.org/citation.cfm?doid=937503.937506.

[28] Shamir, A. (2000). Identity-Based Cryptosystems and Signature Schemes. *Advances in Cryptology*. 196. pp. 47–53.

[29] Sharma, D.K., Saxena, S.K., Sharma, Y. & Tiwari, A. (2009). Identity Based Secure Routing For Wireless Ad-Hoc Networks. *International Journal of Recent Trends in Engineering*. 2 (1). pp. 28–32.

[30] Sharma, R.K., Kishore, N. & Das, P. (2014). Secure and efficient application of MANET using Identity Based cryptography combined with Visual cryptography technique. *International Journal Of Engineering And Computer Science*. 3 (2). pp. 3933–3937.

[31] Sumalatha, P. & Sathyanarayana, B. (2015). Enhanced Identity Based Cryptography for Efficient Group Key Management in WSN. *International Journal of Application or Innovation in Engineering & Management*. [Online]. 4 (6). pp. 116–128. Available from: http://www.ijaiem.org/Volume4Issue6/IJAIEM-2015-06-27-48.pdf.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[32] Sumalatha, P. & Sathyanarayanaa, B. (2015). Enhanced Identity Based Cryptography for Efficient Group Key Management in WSN. *International Journal of Application or Innovation in Engineering & Management*. 4 (6). pp. 116–128.

[33] Wu, B., Wu, J. & Cardei, M. (2008). A Survey of Key Management in Mobile Ad Hoc Networks. In: Y. Zhang, J. Zheng, & M. Ma (eds.). *Handbook of Research on Wireless Security*. Idea Group Inc, pp. 1–23.

[34] Wu, B., Wu, J., Fernandez, E.B., Ilyas, M. & Magliveras, S. (2007). Secure and efficient key management in mobile ad hoc networks. *Journal of Network and Computer Applications*. [Online]. 30 (3). pp. 937–954. Available from: http://linkinghub.elsevier.com/retrieve/pii/S1084804505000524.

[35] Yi, S. & Kravits, R. (2004). Composite key management for ad hoc networks. In: *The First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, 2004. MOBIQUITOUS 2004.* [Online]. 2004, IEEE, pp. 52–61. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1331710.

[36] Yi, S., Naldurg, P. & Kravets, R. (2001). Security-aware ad hoc routing for wireless networks. In: *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing - MobiHoc '01*. [Online]. 2001, New York, New York, USA: ACM Press, p. 299. Available from: http://portal.acm.org/citation.cfm?doid=501416.501464.

[37] Zamani, A.T. & Zubair, S. (2014). Key Management Scheme in Mobile Ad Hoc Networks. *International Journal of Emerging Research in Management &Technology*. 3 (4). pp. 157–165.

[38] Zhao, S., Aggarwal, A., Frost, R. & Bai, X. (2012). A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Networks. *IEEE Communications Surveys & Tutorials*. [Online]. 14 (2). pp. 380–400. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5714975.