International Journal of Civil Engineering and Technology (IJCIET)
Volume 8, Issue 10, October 2017, pp. 99–110, Article ID: IJCIET_08_10_012
Available online at http://http://www.iaeme.com/ijciet/issues.asp?JType=IJCIET&VType=8&IType=10
ISSN Print: 0976-6308 and ISSN Online: 0976-6316

A SURVEY OF INTRUSION DETECTION WITH HIGHER MALICIOUS MISBEHAVIOR DETECTION IN MANET

D. Rajalakshmi
Assistant Professor, Department of Computer Science & Engineering,
Sri Sairam Institute of technology, Chennai, India

Dr. K. Meena
Dr. K. Meena, Associate Professor, Department of Computer Science & Engineering,
Veltech Dr.RR and Dr.SR University

ABSTRACT

The mobile ad hoc networks (MANET) have been used in latest years, in several applications.

They are more susceptible to malicious attack. It's more problematical to deliver security in mobile ad hoc network entirely. It's based on some exclusive characteristics. In addition the inhibition methods need to detect and yield essential activities to deliver the security to these types of networks. For this purpose many intrusion detection systems (IDSs) are used. An Intrusion Detection System (IDS) perceives malicious and selfish nodes in a network. Designing efficient IDS for wireless ad - hoc networks that would not disturb the performance of the network significantly is indeed a challenging task. Detecting Misbehavior (such as transmission of false information) in Mobile Adhoc Network (MANET) is an important problem with wide range of security applications. Authentication and confidentiality is an important aspect of mobile adhoc networks. It enables entities to cope with insecurity and uncontrollability caused by the free will of others. Security management is highly challenging issues in MANETs due to computational complexity constraints, and the independent movement of component nodes. The proposed technique used is Enhanced Adaptive Acknowledgment for intrusion detection system specially designed for MANETs. A Hybrid cryptographic Algorithm is used for obtaining a Authentication of message and recovering the original message without any conflict. The concept of implementing a hybrid scheme in AACK greatly decreases the network overhead.

Keywords: Enhanced Adaptive Acknowledgement (EAACK), Hybrid Cryptographic Techniques, Misbehavior detection, selfish behavior and Mobile Adhoc Networks (MANET).

Cite this Article: D. Rajalakshmi and Dr. K. Meena, A Survey of Intrusion Detection with Higher Malicious Misbehavior Detection in MANET, International Journal of Civil Engineering and Technology, 8(10), 2017, pp. 99–110
http://www.iaeme.com/IJCIET/issues.asp?JType=IJCIET&VType=8&IType=10

1. INTRODUCTION

Wireless ad-hoc networks are playing a prominent role in the rapid deployment of independent mobile users, efficient and dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Ad-hoc networks do not have fix topologies to cover a large area. These topologies may change dynamically and unpredictably. Traditional routing protocols that are normally used for internet based wireless networks. These can't be applied directly to ad-hoc wireless networks; because some common assumptions are not valid in all cases for such dynamically changing networks and may be not true for mobile nodes[16]. The availability of bandwidth is an important issue of ad-hoc networks. Thus, these network types present a difficult challenge in the design of routing protocols, where each node participates in routing by forwarding data dynamically based on the network connectivity. It improves the scalability of wireless networks compared to infrastructure based wireless networks because of its decentralized nature. In critical situations: natural disasters, military conflicts or any emergency moment, ad-hoc networks are best suited due to minimal configuration and quick operation.

Mobile ad hoc networks (MANETs) are infrastructureless, autonomous, stand-alone wireless networks that are receiving growing attention from both academia and industry. Security support is indispensable for typical application scenarios of MANETs such as military and homeland security operations. Security design for MANETs is, however, complicated by a number of unique features of MANETs. Of note are the lack of infrastructure, shared wireless medium, node mobility, resource constraints of mobile devices, bandwidth-limited and error-prone channels, and so on [1].

Figure 1 Mobile Adhoc Networks

Compared with traditional networks, wireless ad hoc networks are more vulnerable to malicious attacks and random failures due to their unique features such as constrained node energy, error-prone communication media, and dynamic network topology. Thus, as pointed out in [11], it is the first major goal for a survivable wireless ad hoc network to establish and maintain a connected topology, whenever it is practical. Based on this observation, as a fundamental topology property and prerequisite for all networking operations, topology connectivity is a critical index for the survivability of wireless ad hoc networks, especially in the presence of malicious attacks and random failures.

Distributed collaborations and information sharing are considered to be essential operations in the MANET to achieve the deployment goals such as sensing and event monitoring. Collaboration will be productive only if all participants operate in a trustworthy manner [1]–[3]. MANETs are usually deployed in harsh or uncontrolled environments, thereby heightening the probability of compromises and malfunctioning as there is no centralized control unit to monitor the node operations. These characteristics force a component node to be cautious when collaborating/communicating with other nodes as the behaviour of nodes change with time and environmental conditions. Therefore, establishing and quantifying behaviour of nodes in the form of trust is essential for ensuring proper operation of MANET. This is particularly important in large scale networks where highly heterogeneous entities participate and high level of collaborations are required e.g., tactical networks with ally nations and social networks [4]. Heterogeneity could be in terms of nodes' operations, sensing capabilities, and other related behaviour.

Trust system can also be used in assessing the quality of received information, to provide network security services such as access control, authentication, malicious node detections and secure resource sharing [5]–[8]. Therefore, it is important to periodically evaluate the trust value of nodes based on some metrics and computational methods.

Trust computations in static networks are relatively simpler because the trust value here changes mainly due to behaviour of nodes. After enough observations these behaviours are predictable. However, in MANET trust computations are challenging because:

- There could be different types of mobility in MANETs such as low mobility (human walking with sensors) or high mobility (mobility of sensors mounted on vehicle). The network composition may significantly change with time in an unpredictable manner due to this mobility. When the neighbour constantly changes, it becomes difficult to make observation and get enough opportunities for interactions to measure the trust. Information received from the MANET nodes are more valuable and trustworthy if they can be related to where and when the readings originated [9]. However, when the location is constantly changing, it is hard to associate the information and node behaviour with locations.
- In the absence of centralized control station, monitoring the behaviour of nodes is very difficult. The complexity in trust computations grows non-linearly without the centralized command center. The worst case complexity of obtaining the trust level on every node by every other node in a network of N connected nodes is O (N2) [10].

2. BACKGROUND & RELATED WORK

A Mobile ad hoc network is a self-configuring dynamic network of mobile devices connected by wireless links with the set for a specific purpose. One of the primary concerns related to ad hoc networks is to provide a secure communication among mobile nodes in a hostile environment. The nature of mobile ad hoc networks poses a range of challenges to the security design. These include an open decentralized peer-to-peer architecture, a shared wireless medium and a highly dynamic topology. The main problem for MANET security resides: the ad hoc networks can be reached very easily by users, but also by malicious attackers. If a malicious attacker reaches the network, the attacker can easily exploit or possibly even disable the mobile ad hoc network.

MANETs are vulnerable in their functionality: intruders can compromise the operation of the network by attacking at any of the physical, MAC or network layers. The network layer, especially the routing protocol, is vulnerable because the use of cooperative routing algorithms, the limited computational ability of nodes, the exhaustible node batteries, a lack of clearly defined physical network boundary and the transient nature of services in the

network. Standard security measures such as encryption and authentication do not provide complete protection, therefore, intrusion detection and prevention (IDP) mechanisms are widely used to secure MANETs.

Intrusion detection (ID) in MANETs is more complex and challenging than in fixed networks, because of the difficulty in fulfilling the requirements and because some characteristics of MANETs create operational and implementation complexities. Additional challenges for IDSs in MANETs are as follows:

- MANETs lacking in concentration points where monitoring and audit data collection can be performed
- MANET routing protocols require nodes to cooperate and act as routers, creating opportunities for attacks
- Due to the nodes' mobility, the network topology is dynamic and unpredictable, making the process of intrusion detection complicated
- IDSs in MANETs are more complex because of the limited computational ability of most of the nodes

Intrusion detection in MANETs, however, is challenging for a number of reasons [16][17][18]. These networks change their topologies dynamically due to node mobility; lack of concentration points where traffic can be analyzed for intrusions; utilize self-configuring multi-party infrastructure protocols that are susceptible to malicious manipulation; and rely on wireless communications channels that provide limited bandwidth and are subject to noise and intermittent connectivity.

To overcome these constraints, researchers have proposed a number of decentralized intrusion detection approaches tailored specifically for MANETs. These approaches, however, have focused almost exclusively on detecting malicious behaviour with respect to MANET routing protocols.

This paper describes a generalized, cooperative intrusion detection architecture proposed as the foundation for all intrusion detection and supporting activities in mobile ad hoc wireless networks.

3. PROBLEM DEFINITION

An intrusion-detection system (IDS) can be defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity. Intrusion detection is typically one part of an overall protection system that is installed around a system or device—it is not a stand-alone protection measure.

Intrusion detection has a bit more history behind it. Endorf [5] stated that the intrusion detection was introduced as a formal research when James Anderson wrote a technical report [6] For the U.S. Air Force. Thus, it has been followed by Denning [7], Heberlein [8], and many researchers until present day. Depending on the detection techniques used, IDS can be classified into three main categories [9] as follows: 1) signature or misuse based IDS), 2) anomaly based IDS, 3) specification based IDS, which it is a hybrid both of the signature and the anomaly based IDS.

The signature-based IDS uses pre-known attack scenarios (or signatures) and compare them with incoming packets traffic. There are several approaches in the signature detection, which they differ in representation and matching algorithm employed to detect the intrusion patterns. The detection approaches, such as expert system [10], pattern recognition [11], colored petri nets [12], and state transition analysis [13] are grouped on the misuse.

- The anomaly-based IDS attempts to detect activities that differ from the normal expected system behavior. This detection has several techniques, i.e.statistics [14], neural networks [15], and other techniques such as immunology [16], data mining [[18[, [19]], and Chi-square test utilization [17]. Moreover, a good taxonomy of wired IDSes was presented by Debar [20].
- The specification-based IDS monitors current behavior of systems according to specifications that describe desired functionality for security-critical entities [21]. A mismatch between current behavior and the specifications will be reported as an attack.
- The different characteristics of MANET includes lack of centralized administration, limited resources, dynamically changed network topology, wireless communication, limited power, limited bandwidth etc. Due to these features, mobile ad hoc networks are more vulnerable to attacks.
- Dynamic Topology: Ad hoc networks require complicated routing protocols. Misbehaving node can generate wrong routing information which is very tough to discover. The devices' mobility also causes a problem.
- Lack of Infrastructure: Ad hoc networks do not have any fixed infrastructure or centralized coordination. Therefore the traditional security mechanisms such as cryptography and certification are inapplicable. Susceptibility of nodes: Physical protection of nodes is not possible. Hence they can be captured more easily and falls under the control of an attacker.
- Susceptibility of channels: In wireless network, message eavesdropping and injection of fake messages into the network is easy without having physical access to network components. Denial of service also applicable.

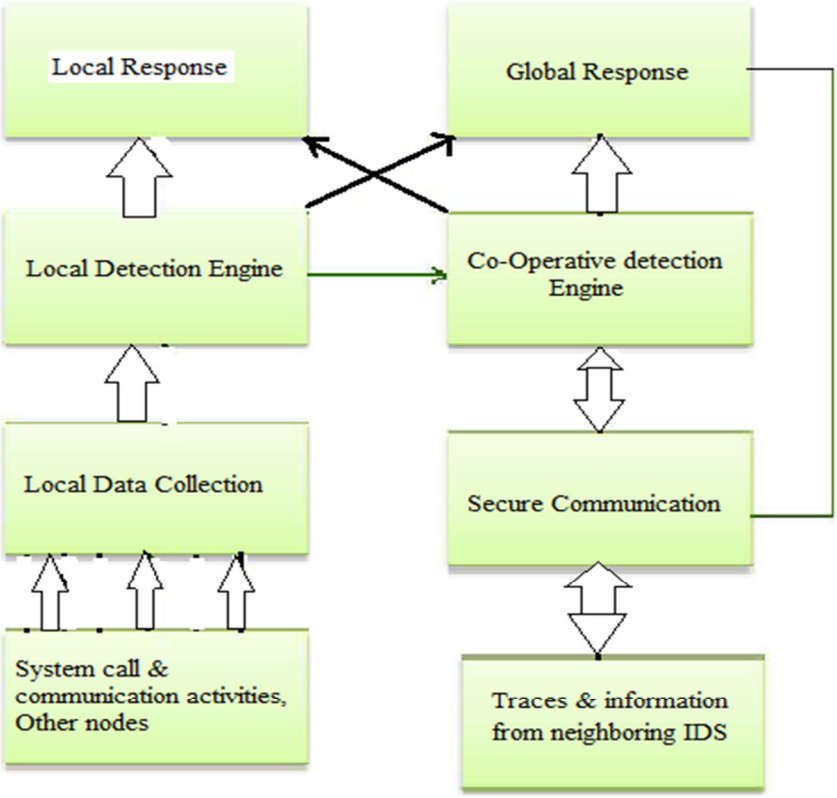

Figure 2 A Conceptual Model for IDS

4. PROPOSED SYSTEM

Protecting access to information for reasons of security is still a major reason for using cryptography. However, it's also increasingly used for identification of individuals, for authentication and for non-repudiation. This is particularly important with the growth of the Internet, global trading and other activities[39]. The identity of e-mail and Web users is trivially easy to conceal or to forge, and secure authentication can give those interacting remotely confidence that they're dealing with the right person and that a message hasn't been forged or changed. In commercial situations, non-repudiation [38] is an important concept ensuring that if, say, a contract has been agreed upon one party can't then renege by claiming that they didn't actually agree or did so at some different time when, perhaps, a price was higher or lower. Digital signatures and digital timestamps are used in such situations, often in conjunction with other mechanisms such as message digests and digital certificates.

The range of uses for cryptography and related techniques is considerable and growing steadily. Passwords are common but the protection they offer is often illusory, perhaps because security policies within many organizations aren't well thought out and their use causes more problems and inconvenience than seems worth it[38,40]. In many cases where passwords are used, for example in protecting word processed documents, the ciphers used are extremely lightweight and can be attacked without difficulty using one of a range of freely available cracking programs.

- A hybrid encryption is a combination of more than one cryptographic algorithm
- It provides more security.
- It incorporates a combination of asymmetric and symmetric encryption
- Hybrid encryption is considered a highly secure type of encryption as long as the public and private keys are fully secure.

Encryption Steps using Hybrid Crypto System at the Source

- source has destination public key(PUK)
- Inputs: Plain Data Block (PDB) Symmetric Key (SK)
- Outputs: Encrypted Data Block *(EDB)*
- EDB contains both the encrypted PDB (denoted by ED) concatenated with encrypted SK (denoted by ESK)

Encryption Steps:

1) Encrypt PDB using SK to get ED.
2) Encrypt SK using destination's PUK to get ESK.
3) Concatenate ED with its corresponding ESK to get EDB which is sent to the destination. EDB = { ESK , ED }

Decryption Steps using Hybrid Crypto System at the Destination

Prerequisite: Destination has its Private Key (PRK)

Inputs: Encrypted Data Block (EDB)

Note: EDB contains both the encrypted PDB (denoted by ED) concatenated with encrypted SK (denoted by ESK)

Outputs: Plain Data Block (PDB)

Decryption Steps:

1) Decrypt ESK using PRK to retrieve SK
2) Use the retrieved SK as decryption key to decrypt ED to get PDB.

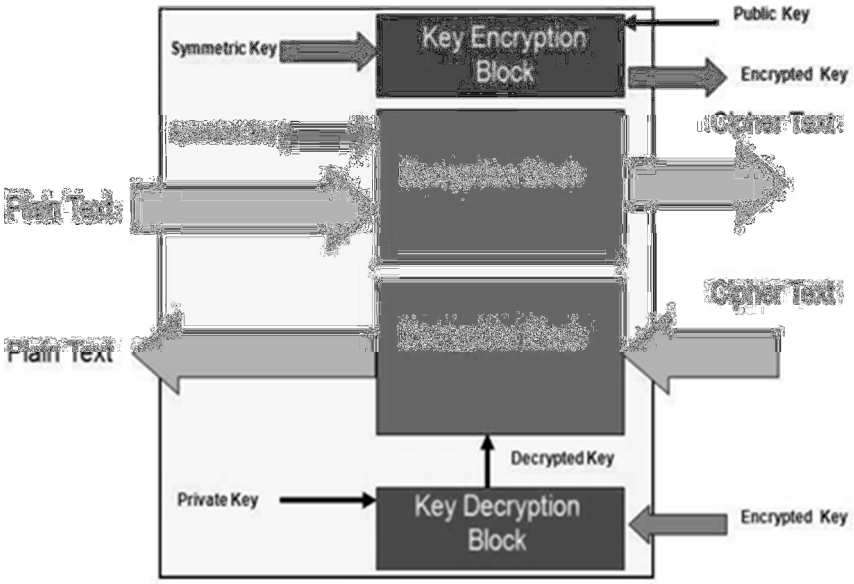

Figure 3 Block diagram of hybrid crypto system

There is no explicit key transfer in the hybrid crypto system our proposed key exchange works in the manner shown in Fig.4

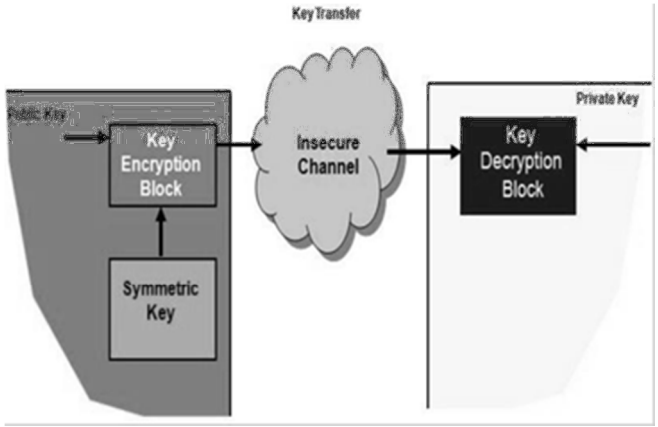

Figure 4 Key transfer using hybrid crypto system

HYBRID CRYPTO SYSTEM USING RSA AND D-H

Steps of this algorithm are as

1. Choose two large prime numbers P and Q.

a) Calculate N = P x Q.

b) Select public key (i.e. encryption key) E such that it is not a factor of (p-1) and (q-1)

c) Select the private key (i.e. the decryption key) D such that the following equation is true (D x E) mod (P – 1) x (Q – 1) = 1

Suppose R, S and G is automatic generated prime constants And put A=E and B=D

Now calculate following as public number $X= G^A \bmod R$ $Y= G^B \bmod R$

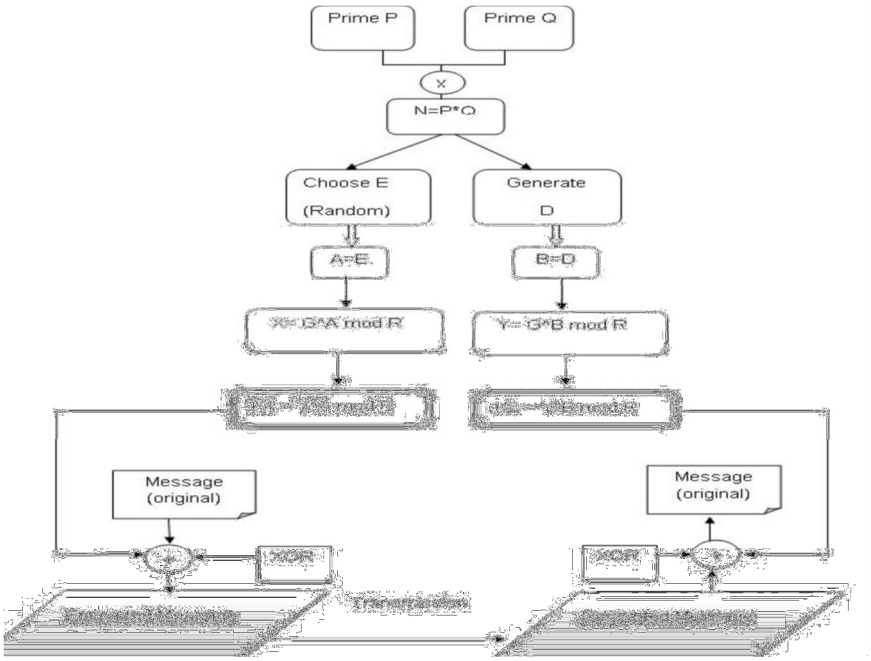

Figure 5 A hybrid RSA & Diffie Hellman

3. Calculate session key with formula

$$K_A = Y^A \bmod R \quad K_B = X^B \bmod R$$

$$\text{Such that } K_A = K_B = K.$$

In this section, we describe our proposed EAACK scheme in detail. The approach described in this research paper is based on our previous work, where the backbone of EAACK was proposed and evaluated through implementation. In this paper, we extend it with the introduction of hybrid cryptography techniques to prevent the attacker from forging acknowledgment packets.

A. ACK

ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. In Fig. 8, in ACK mode, node S first sends out an ACK data packet Pad1 to the destination node D. If all the intermediate nodes along the route between nodes S and D are cooperative and node D successfully receives Pad1, node D is required to send back an ACK acknowledgment packet Pak1 along the same route but in a reverse order.

B. S-ACK

The S-ACK scheme is an improved version of the TWOACK scheme proposed by Liu et al. The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node

C. MRA

The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The false misbehavior

report can be generated by malicious attackers to falsely report innocent nodes as malicious. This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route.

D. Hybrid Cryptography Techniques

EAACK is an acknowledgment-based IDS. All three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely on acknowledgment packets to detect misbehaviors in the network. Thus, it is extremely important to ensure that all acknowledgment packets in EAACK are faithful and uncorrupted. If the intruders are smart abundant to fake acknowledgment packets, all of the three schemes will be susceptible. With regard to this crucial concern, we developed hybrid cryptographic techniques in our proposed scheme. To ensure the integrity of the IDS, EAACK requires all acknowledgment packets to be delivered after verifying the sender and receiver key information.

5. CONCLUSION

In this survey paper, a Secure Intrusion Detection with higher malicious misbehaviour nodes detection and attacks on MANETs will demonstrate to be a virtuous solution for redeemable resources in the Real time environment. To provide security the hybrid cryptography techniques is presented that utilizes both symmetric key and public key cryptographic algorithms & Enhanced Adaptive Acknowledgement has been developed for better performance in terms of computation costs and memory storage requirements. Therefore, IDS has become an indispensable component to provide defence – in – depth security mechanisms for MANETs.

REFERENCES

[1] Sushmita Ruj, Marcos Antonio Cavenaghi, Zhen Huang, Amiya Nayak, and Ivan Stojmenovic. Data-centric misbehavior detection in vanets. ArxivarXiv:1103.2404v1, 2011.

[2] R. H. Akbani, S. Patel, and D. C. Jinwala, ―DoS attacks in mobile ad hoc networks: A survey,‖ in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012, pp. 535– 541.

[3] K. Stanoevska-Slabeva and M. Heitmann, ―Impact of mobile ad-hoc networks on the mobile value system,‖ in Proc. 2nd Conf. m-Bus., Vienna, Austria, Jun. 2010

[4] R. Akbani, T. Korkmaz, and G. V. S. Raju, ―Mobile Ad hoc Network Security, in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[5] A. Tabesh and L. G. Frechette, A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micro power generator, IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 840–849, Mar. 2010.

[6] Elhadi M.Shakshuki, Nan Kang and Tarek R.Sheltami, EAACK – A Secure Intrusion Detection System for MANETs‖ in Industrial Electronics, Vol 60, No.3, 2013.

[7] N. Kang, E. Shakshuki, and T. Sheltami, Detecting misbehaving nodes in MANETs, in Proc. 12th Int. Conf. iiWAS, Paris, France, Nov. 8–10, 2010, pp. 216–222.

[8] N. Kang, E. Shakshuki, and T. Sheltami, Detecting forged acknowledgements in MANETs, in Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.

[9] S. Hashmi and J. Brooke, Toward Sybil resistant authentication in mobile ad hoc networks,‖ in Proc. 4th Int. Conf. Emerging Security Inform., Syst. Technol., 2010, pp. 17–24.

[10] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, Detecting and localizing identity-based attacks in wireless and sensor networks, IEEE Trans. Veh. Technol., vol. 59, no. 5, pp. 2418–2434, Jun. 2010.

[11] R. Akbani, T. Korkmaz, and G. V. S. Raju, Mobile Ad hoc Network Security, in Lecture Notes in Electrical Engineering, vol. 127.New York: Springer-Verlag, 2012, pp. 659–666.

[12] F. Xing and W. Wang, Modeling and Analysis of Connectivity in Mobile Ad Hoc Networks with Misbehaving Nodes, Proc. IEEEInt'l Conf. Comm. (ICC '06), pp. 1879-1884, June 2006.

[13] F. Anjum and P. Mouchtaris, Security for Wireless Ad Hoc Networks. John Wiley and Sons, Inc., 2007.

[14] T. Anantvalee and J. Wu, A Survey on Intrusion Detection in Mobile Ad Hoc Networks, Wireless/Mobile Network Security, Springer, 2006.

[15] H. Otrok, N. Mohammed, L. Wang, M. Debbabi, and P.Bhattacharya, A Game-Theoretic Intrusion Detection Model for Mobile Ad-Hoc Networks, J. Computer Comm., vol. 31, no. 4, pp. 708-721, 2008.

[16] Y. Zhao, W. Liu, W. Lou, and Y. Fang, Securing mobile ad hoc networks with certificate less public keys, IEEE Trans. Dependable Secure Comput., vol. 3, no. 4, pp. 386–399, Oct.–Dec. 2006.

[17] B. Rong, H.-H. Chen, Y. Qian, K. Lu, R. Q. Hu, and S. Guizani, A pyramidal security model for large-scale group-oriented computing in mobile ad hoc networks: The key management study, IEEE Trans. Veh. Technol., vol. 58, no. 1, pp. 398–408, Jan. 2009.

[18] J. Liu, F. R. Yu, C.-H. Lung, and H. Tang, Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks, IEEE Trans. Wireless Commun., vol. 8, pp. 806–815, Feb. 2009.

[19] Mainak Ghosh, Anitha Varghese, Arobinda Gupta, Arzad Alam Kherani, and Skanda N. Muthaiah. Detecting misbehaviors in vanet with integrated root-cause analysis. Ad Hoc Networks, 8(7):778–790, 2010.

[20] Soyoung Park, Baber Aslam, Damla Turgut, and Cliff C. Zou. Defense against sybil attack in vehicular ad hoc network based on roadside unit support. In MILCOM, pages 1-7, 2009.

[21] G. A. Jacoby and N. J. Davis, Mobile host-based intrusion detection and attack identification, IEEE Wireless Commun., vol. 14, pp. 53–60, Aug. 2007.

[22] W. Lou and Y. Fang, A Survey of Wireless Security in Mobile AdHoc Networks: Challenges and Available Solutions, Ad-HocWireless Networking, X. Chen, X. Huang, and D.-Z. Du, eds., Kluwer Publisher, Mar. 2003.

[23] R. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1983.

[24] J. G. Rocha, L. M. Goncalves, P. F. Rocha, M. P. Silva, and S. Lanceros- Mendez, Energy harvesting from piezoelectric materials fully integrated in footwear, IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 813–819, Mar. 2010.

[25] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, Video transmission enhancement in presence ofmisbehaving nodes inMANETs, Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282, Oct. 2009.

[26] A. Singh, M. Maheshwari, and N. Kumar, Security and trust management in MANET, in Communications in Computer and Information Science, vol. 147. New York: Springer-Verlag, 2011, pt. 3, pp. 384–387.

[27] B. Sun, Intrusion detection in mobile ad hoc networks, Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.

[28] K. Stanoevska-Slabeva and M. Heitmann, Impact of mobile ad-hoc networks on the mobile value system, in Proc. 2nd Conf. m-Bus., Vienna, Austria, Jun. 2003.

[29] A. Tabesh and L. G. Frechette, A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micro power generator, IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 840–849, Mar. 2010.

[30] M. Zapata and N. Asokan, Securing ad hoc routing protocols, in Proc. ACM Workshop Wireless Secur., 2002, pp. 1–10.

[31] L. Zhou and Z. Haas, Securing ad-hoc networks, IEEE Netw., vol. 13, no. 6, pp. 24–30, Nov./Dec. 1999.

[32] Botan, A Friendly C ++ Crypto Library. [Online]. Available: http:// botan.randombit.net/

[33] Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS).

[34] TIK WSN Research Group, The Sensor Network Museum-Tmote Sky. [Online]. Available: http://www.snm.ethz.ch/Projects/TmoteSky

[35] 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.

[36] T. Anantvalee and J. Wu, A Survey on Intrusion Detection in Mobile Ad Hoc Networks, in Wireless/Mobile Security. New York: Springer- Verlag, 2008.

[37] L. Buttyan and J. P. Hubaux, Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[38] B. den Boer and A. Bosselaers, Collisions for the compression function of MD5‖, Advances in Cryptology, Eurocrypt 07, pages 293-304, Springer-Verlag, 2007.

[39] D. Bleichenbacher and A. May, New attacks on RSA with small CRTexponent in Public Key Cryptography, PKC 2006, volume 3968 of Lecture Notes in Computer Science, pages 1–13. Springer-Verlag, 2006.

[40] D. Bleichenbacher and A. May, New attacks on RSA with small secret CRT-exponents, in Public Key Cryptology-PKC 2006, ser. Lecture Notes in Computer Science. New York: Springer, 2006, vol. 3958, pp. 1–13.

[41] N. Kang, E. Shakshuki, and T. Sheltami, Detecting misbehaving nodes in MANETs, in Proc. 12th Int. Conf. iiWAS, Paris, France, Nov. 8–10, 2010, pp. 16–222.

[42] N. Kang, E. Shakshuki, and T. Sheltami, Detecting forged acknowledgements in MANETs, in Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.

[43] K. Kuladinith, A. S. Timm-Giel, and C. Görg, Mobile ad-hoc communications in AEC industry, J. Inf. Technol. Const., vol. 9, pp. 313–323, 2004.

[44] J.-S. Lee, A Petri net design of command filters for semiautonomous mobile sensor networks, IEEE Trans. Ind. Electron., vol. 55, no. 4, pp. 1835–1841, Apr. 2008.

[45] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, An acknowledgment-based approach for the detection of routing misbehavior in MANETs, IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[46] S. Marti, T. J. Giuli, K. Lai, and M. Baker, Mitigating routing misbehaviour in mobile ad hoc networks, in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., Boston, MA, 2000, pp. 255–265.

[47] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL: CRC, 1996, T-37.

[48] N. Nasser and Y. Chen, Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network, in Proc. IEEE Int. Conf. Commun., Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159.

[49] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, On intrusion detection and response for mobile ad hoc networks, in Proc. IEEE Int. Conf. Perform., Comput., Commun., 2004, pp. 747–752.

[50] A. Patcha and A. Mishra, Collaborative security architecture for black hole attack prevention in mobile ad hoc networks, in Proc. Radio Wireless Conf., 2003, pp. 75–78.

[51] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, Secure routing and intrusion detection in ad hoc networks, in Proc.3rd Int. Conf. Pervasive Comput. Commun., 2005, pp. 191–199.

[52] V. C. Gungor and G. P. Hancke, Industrial wireless sensor networks: Challenges, design principles, and technical approach, IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[53] Y. Hu, D. Johnson, and A. Perrig, SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks, in Proc. 4th IEEE Workshop Mobile Comput. Syst. Appl., 2002, pp. 3–13.

[54] Y. Hu, A. Perrig, and D. Johnson, ARIADNE: A secure on-demand routing protocol for ad hoc networks, in Proc. 8th ACM Int.Conf. MobiCom, Atlanta, GA, 2002, pp. 12–23.

[55] 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.

[56] D. Johnson and D. Maltz, Dynamic Source Routing in ad hoc wireless networks, in Mobile Computing. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[57] Sajani J and Dr. S. Manikandan, Analysing and Monitoring of Network IDS Using Intrusion Detection. International Journal of Computer Engineering & Technology, 8(3), 2017, pp. 20–27.

[58] Bejoy B J and Dr. Janakiraman S, Artificial Immune System Based Intrusion Detection Systems- A Comprehensive Review. International Journal of Computer Engineering & Technology, 8(1), 2017, pp. 85–95.

[59] V. Jaiganesh, Dr. P. Sumathi, An Efficient Intrusion Detection Using Relevance Vector Machine, International Journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 1, January- February (2013), pp. 383-391

[60] Syeda Gauhar Fatima, Dr. Syed Abdul Sattar and Dr. K. Anita Sheela, Energy Efficient Intrusion Detection System for Wsn, International Journal of Electronics and Communication Engineering & Technology (IJECET), Volume 3, Issue 3, October-December (2012), pp. 246-250