AENSI Journals

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Malicious Behaviour of Node and its Significant Security Techniques in MANET-A Review

Burhan Ul Islam Khan, Rashidah Funke Olanrewaju, Mohamed Hadi Habaebi

Department of Electrical and Computer Engineering, Kulliyyah of Engineering; International Islamic University, Malaysia

ARTICLE INFO

Article history:
Received 23 October 2013
Received in revised form 17 November 2013
Accepted 23 November 2013
Available online 4 December2013

Keywords:t
Attacks
Mobile Adhoc Network Malicious Node
Nuglets
Security threats

ABSTRACT

Mobile adhoc network is one of the major discussed topic in the field of wireless network and communication system from past few decades. Various extensive research work conducted in the past shows that mobile adhoc network is shrouded with various type of issues e.g. dynamic topologies, inefficient routing policies, unwanted energy depletion, and security. Although various solutions has been explored for addressing other issues in MANET, but solutions previously introduced for mitigating security threats in MANET are yet to be standardized or found robust enough. One of the root causes for the same is that there is a tremendous amount of unpredictability in the behavior of the mobile nodes in MANET, be it regular node or erroneous node or malicious node. Hence, this paper discusses only the significant research work that has been introduced in the past for the purpose of mitigating security threats in MANET.

To Cite This Article: Burhan Ul Islam Khan, Rashidah Funke Olanrewaju, Mohamed Hadi Habaebi Malicious Behaviour of Node and its Significant Security Techniques in MANET-A Review**.** ***Aust. J. Basic & Appl. Sci.,*** *7(12): 286-293, 2013*

INTRODUCTION

In modern era of advanced networking and communication system, mobile adhoc network (MANET) has increasingly attracted many researchers and academicians for its strong benefits in the line of infrastructure independent communication system. Such type of the infrastructure independent network basically possesses a large number of mobile nodes that paves a communication link with other mobile nodes and thereby gives rise to various mobile applications (Hoebeke *et al*, 2004). The security of the MANET system is shrouded with various security loopholes e.g. absence of infrastructure, resource limitation, restricted physical security, and obvious root-factor i.e. dynamic topology. It has been realized from the prior work (Visalakshi *et al*, 2012), (Chen *et al*, 2009), (Cordasco *et al*, 2008) that cryptographic techniques are frequently considered and prioritized in majority of the security approaches in MANET. In sturdy association with mathematical theories, cryptographic techniques are quite challenging to design without enough researches and excavating the security analysis of MANET (Pellegrino *et al*, 2006). One of the cost effective procedure to identify the possible optimal solution against security in MANET is to investigate the previous research work that claims cryptographic-techniques as a solution of security. The prime aim of adopting such step would be an attempt to discover an effective as well as robust security approach that is computationally efficient and can ensure better scalability, optimized network performance, less storage etc. (Pellegrino *et al*, 2006). Conventionally speaking, cryptographic techniques have been witnessed to be frequently used in providing security solution especially in wireless environment of adhoc network where the vulnerability against intrusion is always maximized. Hence, it can be said that there was a wide usage of superior and robust encryption techniques in the past that makes sure that there is a privacy and confidentiality in the established session between the communicating nodes. It was also seen that majority of the previous study has discussed cryptography as a solution to mitigate various security breaches in MANET (Wu, 2008), (Pervaiz *et al*, 2008). With such a wide range of study, it has become more challenging task that whether cryptographic technique should be adopted in future for promising security. The prime reason behind this is higher computational complexity associated with advanced cryptographic techniques.

Another fundamental challenge of security formulation is the dynamic topology and decentralized nature of MANET system. This unpredictable scenario in selection by routing protocols for communication system in MANET gives rise to one of the peak security issue i.e. authenticating genuine node as well as malicious nodes.

Corresponding Author: Burhan Ul Islam Khan, International Islamic University Malaysia, Kulliyyah of Engineering, Department of Electrical & Computer Engineering. P.O. Box. 53100. Kuala Lumpur. Malaysia. Tel +60183140768 E-mail: burhan.iium@gmail.com

Australian Journal of Basic and Applied Sciences, 7(12) Oct 2013, Pages: 286-293

The presence of malicious node of any types is always potentially harmful to any MANET application and has wide spread damage of the computing resources connected in MANET.

Not only cryptography, there are some other schemes also being witnessed in the past literatures claiming to be robust security measures against some of the potential threats in MANET. However, evaluation of all these techniques is yet to be seen as MANET is basically susceptible to different types of attacks that deteriorates the trust factor and corrupts the reputation system thereby infecting the massive part of the wireless environment. Hence, inspite of investigating the solution by using cryptography or some other relevant techniques, it is critical to understand the malicious and selfish behaviour of a node and their abnormal patterns exhibited in the networking scenario of MANET. Because of this fact, IDS system fails as such types of malicious nodes always can be smart enough to bypass their security protocols and inflict more potential attack on the environment.

The prime purpose of this paper is to review the most standard and effective techniques introduced in the past which are frequently considered for securing MANETs. The article will elaborate that how far the techniques discussed by the previous researchers resist the most lethal attacks in MANET. Section 2 provides an overview of malicious node behavior. Section 3 explores various security solutions that have been put forth in the literature to thwart the malicious behavior. Finally, section 4 makes some concluding remarks.

Understanding Malicious Behaviour:

From the networking viewpoint, in mobile adhoc networks (MANET), every individual intermediate node is considered to forward the data packets to its neighbor nodes such that it reaches its destination owing to its mobility. This characteristics of MANET is found to be common in majority of routing protocols as defined by RFCs(Junhai *et al*,2009). However, due to scarcity of enough resources, this characteristics are found to malfunction sometimes that eventually leads to the evolution of selfish nodes (Yoo *et al*, 2006). The previous record of studies (Miranda *et al*, 2003) shows that various attempts has been made to make sure the selfish node doesn't exist much and even if it exist also, the routing protocols are amended using various incentive techniques for ensuring forwarding of data packets. Although such techniques are quite successful formulating tactics of managing selfish nodes in the environment of MANET, however, such tactics couldn't successfully justify or result in promising results that could accomplish the ultimate effective routing policies and maximize QoS throughput. The wireless nature of environment of MANET actually makes the network more vulnerable and susceptible to various types of attacks which are further boosted by open architecture of MANET system (Jiang *et al*, 2007). One of the prominent secure strategies formulated in past studies is by deploying secure routing protocols (Striki *et al*,2008). Unfortunately, the disadvantage explored even in the secure routing protocols in the past is that they are accompanied by extensive computational overhead that has exponential adverse effect on the efficiency of communication system in MANET (Striki *et al*,2008).

One of the prime targets of the intruder in MANET is to victimize the routing process and thereby affect the entire communication system by not obeying the secure specifications of routing protocols. This fact is further made worst by the dynamic topology and decentralized nature of MANET that welcomes majority of the attacks in such vulnerable wireless atmosphere (Batra *et al*, 2010). One of the most challenging issues in identification process of malicious node is that the nature of attacking policies are extremely hard to determine as MANET doesn't have enough security system in their policies. The secondary challenges in the identification process of malicious activities are lack of systematic network surveillance process due to lack of centralized system especially in large scale environment (Batra *et al*, 2010). Attacks on a frequently used routing protocols like AODV and DSDV are studied in (Zapata *et al*,2002), (Hu *et al*, 2005) and (Singh *et al*,2011). One of the major discrepancies in all the above mentioned studies are that at any cost, even to a little extent, the intruder node is always successful to block the packet forwarding activities of regular node and thereby they gain a advantage factor at the cost of other regular nodes. All the intrusion studies mentioned above are highly capable enough to intrude the regular node, capturing the data, corrupts and disrupts the routes, leading to compromization of the entire large scale environment of MANET system. This fact is really scary when it comes to real time usage of MANET for any specific commercial applications. Hence, in a nutshell, it can be said that malicious behaviour of MANET is something which is very hard to investigate due to the complex design of attack policies and inherent characteristics of MANET that accelerates the entire vulnerable situation.

Hence, this section after reviewing the work of (Saini *et al*, 2011) will attempt to illustrate the realistic definition of malicious and normal behaviour of MANET.

- Regular Node Behaviour: One of the concrete image of regular node is to forward the data packet from source node to destination node via intermediate node at any cost. While performing packet forwarding, the process of communication is also characterized by security protocols which maintain optimal integrity, confidentiality, authenticity, availability, and non-repudiation.
- Malicious Node Behaviour: A malicious node always performs certain activity which is always harmful for the wireless environment at any cost. Following are the consequences that results in eventual behaviour of malicious nodes:

- Buffer Overflow: The compromised node can saturate the buffer using counterfeited route updates and hence paralyze the neighbor network.
- Bandwidth Usage: The malicious node or the compromised node highly consumes the channel capacity leading to unnecessary traffic blockage, an ideal environment to initiate more potential attacks.
- Energy Usage: The malicious/compromised node exponentially uses energy for performing re-transmission and other unwanted operations.
- Eavesdropping: One of the frequently used preliminary techniques that attempt to drop the packet and compromise the network.
- Intermittent Link: The malicious node using the above mentioned operations blocks the communication between a sender and recipient node leading to link breakage.
- Delay: Due to intermittent link, the duration of forwarding the data packets by regular node is delayed towards its destination.
- Tampering data packets: One of the potential operations of malicious node is to change the sensitive information and embed forged information in the message.
- Bypass authentication: It is easier for malicious node to circumvent any types of network authentication mechanism.
- Capturing Session: One of the most lethal operations of malicious node is to excavate the established session between the regular nodes and steal the information transmitted within the ongoing session.

Hence, it can be seen that defining a malicious behaviour is a very challenging task that calls for identifying either of the one consequence discussed above. All the operations are actually interconnected to each other which is why providing the solution towards security is multi-dimensional problem in Mobile Adhoc Network.

Countermeasures Against Malicious Behaviour:

The previous section has just witnessed the possible behavioral pattern of malicious nodes. This section discusses in brief about prominent security approaches that has been evolved in the past research work as following.

A. Security through Cryptography:

Majority of the security protocols in mobile adhoc network is designed based on cryptographic (William *et al*, 2006) measures. The basic tactics of cryptography is to encrypt the sensitive data into the indecipherable format which will be somewhat impossible for the intruder to access the prime contents of it. The encryption is done either using symmetric way (which uses same key to encrypt and decrypt the data) or using asymmetric way (which uses one key to encrypt and other to decrypt the data) and thereby preserving the confidentiality and integrity of the original data by adopting various algorithms e.g. SHA (Secure Hash Algorithm), MD5 (Message Digest 5), MAC (Message Authentication Codes), and Digital Signature. The prominent cryptographic techniques used in mobile adhoc network are tabulated in Table 1as follows:

B. Security through Trusted Third Party:

In the area of Mobile Adhoc Network from the viewpoint of security, the term 'trust' is something extremely critical parameter to be designed for fetching perfection. The process of estimating trust factor can be used for the purpose of authenticating communication between nodes, permitting controls over routing, and thereby performs secure communication (Li *et al*, 2005). Unfortunately, performing investigation and thereby formulating trust factor is one of the prominent security issues due to inherent characteristics of MANET. Usually in traditional static wireless networking system, usage of trusted third party is very common as it acts as a central point of authentication for furnishing secure communication system. However, it is not possible in dynamic MANET due to its decentralized nature. Hence, previous research work has witnessed evolution of a secure technique by introducing trusted third party in MANET for enhancing security measure. One of the notable work can be found in (Adams *et al*,1999), where the certificate authority or commonly known as CA is considered as trusted third party that issues a certificate to the genuine node for the purpose of authentication during communication procedure. Advantage of this technique is that the system can effectively preserve the authentication policy in third party which is difficult for the intruder to hack inside.

Similar category of the work can be seen in (Patcha *et al*, 2003) where the author has introduced a '*watchdog*' node as trusted third party that surveil the availability of node. The advantage point of this technique is that the '*watchdog*' node actually performs security check of the data packet that is being forwarded by the sender to the destination node via intermediate node. Also, the author in (Panos *et al*, 2010) has presented '*Random Walker Detector*' as trusted third party that evaluates granularity of node operations to survey its vulnerable condition.

C. Security through Intrusion Detection Systems:

The prime goal of intrusion detection system (IDS) in adhoc netwSorks is to surveil the malicious activities and identify the potential threats (Intrusion Detection Systems.(2003).. This section discusses some of the prominent IDS techniques that have been deployed in the past for securing MANET.

Table 1: Overview of cryptographic techniques used in security schemes in MANETs [5].

Scheme	Security Objectives	Techniques
ARAN, (Sanzgiri *et al*, 2002)	Authentication, integrity, and non-repudiation of signaling packets, based on AODV (Perkins, 2001), designed to substitute reactive routing protocols	Certificate Authority, timestamp
ARIADNE (Hu *et al*, 2005)	Authentication and integrity of signal packets, based on the basic operations of DSR (Perkins, 2001).	Symmetric cryptography primitives, hash function and timestamp
SAODV (Lu *et al*, 2009)	Authentication and integrity of signaling packets, a security extension for AODV.	Digital signature and Hash chain
SEAD (Hu *et al*, 2005)	Authentication and integrity of signaling packets, based on DSDV (Perkins, 2001), applied to other distance vector protocols.	Hash chain and Sequence Number
LEAP (Zhu *et al*, 2004)	Source and message one way key chain based authentication and cluster-based shared key in key management to countermeasure wormhole, sinkhole, Sybil, DoS, replay, insider attacks.	Hash chain and Cluster-based shared key.
SLSP (Papadimitratos *et al*, 2003)	Authentication, integrity, and non-repudiation of signal packets, extends an intra-zone protocol for ZRP (Perkins, 2001).	Certificate authority
SPAAR (Carter *et al*, 2003)	Authentication, integrity, non-repudiation, and confidentiality, secure position aided ad hoc routing protocol.	Certificate authority and timestamp.
SOLSR (Adjih *et al*, 2003)	Authentication and integrity of signaling packets.	MACs and timestamp.
SHELL (Younis *et al*, 2006)	A cluster-based key management scheme. Each cluster has its own distributed key management entity residing in a-cluster-head node. Therefore, the operational responsibility and key management responsibility are separated, which offers better resiliency against node capture.	Group shared key.
LHAP (Zhu *et al*, 2003)	A hop-by-hop authentication protocol for adhoc networks.	Digital signature
IKM (Zhang *et al*, 2006)	Key management to secure mobile ad hoc network, efficient network-wide key update via a single broadcast message.	ID-based and threshold cryptography
IBV (Zhang *et al*, 2008)	An efficient batch signature verification scheme for vehicular sensor networks.	Batch verification of ID-based signature.

- ***Credit-Based Methods:***

(Koshti *et al*, 2011) have surveyed some of the credit based techniques for resisting selfish characteristics in mobile adhoc network. Such system usually encourages the selfish node by attaching an incentive for the purpose of forwarding a data packet to its neighbor nodes. Usually, credit based techniques are performed by i) packet purse model and ii) packet trade model. In packet purse model, the owner of the data packet needs to pay the incentive for forwarding it and in packet trade model, the packet forwarding services are negotiated by various nodes ensuring some of the nodes to forward the packet. The prominent advantage of this method is that it allows effective usage of incentives only in case any nodes (selfish) chose to forward the message. However, these techniques are also accompanied by some shortcomings of selection of the nodes which is not in control of the originator of the message. Although, this secure policy has less network overhead, but it is also shrouded by uncertainty of effectiveness in selection of forwarding services by the selfish nodes. Various other credit based schemes are tabulated in Table 2:

- ***Reputation-Based Methods:***

These types of methods usually evaluate reputation by estimating direct interaction with the mobile nodes and/or indirect data gathered from neighbor nodes. Such techniques are adopted especially for authentication purpose where reputation can be evolved on each node (Abbas *et al*, 2010). Various methods of reputation based schemes are tabulated in Table 3.

D. Security through Secure Protocols:

Multiple security protocols have been discussed in the past that are intended to furnish security to the network. Protocols like SEAD (Hu *et al*, 2005), ARAN (Sanzgiri *et al*, 2002), SAAODV (Lu *et al*, 2009) are the example of secure protocols. Such protocols are developed with the idea of cryptography, certification system, and other security solutions. Table 1 highlights some of the frequently used security techniques that use security protocols.

Australian Journal of Basic and Applied Sciences, 7(12) Oct 2013, Pages: 286-293

E. Others Security Techniques:

Various other frameworks and security algorithms have been presented in the past that ensure detecting and preventing the malicious behavior of nodes. Such methods constitute the concept of above security solutions like certification system cryptography, intrusion detection system, etc.

- Security using Genetic Algorithm: (Nikhil *et al*, 2012) has used a genetic algorithm as an optimization technique for performing routing in MANET. The results show that, with the genetic algorithmic technique each cluster-head handles the maximum possible numbers of mobile nodes in its cluster in order to facilitate the optimal operation of the medium access control (MAC) protocol. One of the prominent disadvantages of the study is that the consideration of the fitness function has been done without considering any mitigation for new types of attacks. Hence, the result doesn't ensure robustness against majority of the lethal attacks in MANET
- Security using Artificial Neural Network: (Vishwanath *et al*, 2010) have identified security issues affecting the routing in mobile adhoc Networks and have proposed routing schemes using Artificial Neural Network to Secure Multicasting in MANET's. Although the simulation results are optimal in the defined case, but increase of node leads to increase of training phase in neural network leading to computational overhead.
- Security using Support Vector Machine: (Sharma *et al*, 2013) have presented network traffic predictive method based on the Least Squares SVM. The usage of SVM in this case ensures better training scenario, however, it doesn't ensures security if the attack model is changed.
- Security using Swarm Intelligence: The authors (Kadri *et al*, 2013) have presented security measures that use Ant Colony Optimization using public key infrastructure to design a secure routing protocol. Although the authors have established a robust data confidentiality using a session key and performed analysis on various types of attacks, but still the behaviour pattern of malicious node is not focused in detail.
- Security using Game Theory: (WANG *et al*, 2012) have presented a global punishment-based repeated-game model and investigate the equilibrium conditions of packet forwarding strategies when the whole network is in a cooperative state. This framework takes node rationales into consideration. The accomplished result shows promising probability of promoting node forwarding mechanism. However, various consideration of malicious activity could be more effectively designed if attacker module would have been enhanced.

Hence, it can be clearly seen that although in past decade, multiple solution has been proposed by various researchers with the aim of securing communication system in MANET, but, it can be seen that almost every solutions is tagged with security loopholes that has either not considered an appropriate experimental test bed, or have not considered a wide range of attack. Even if some of the results are potentially secure, but it is found with QoS issues too. Therefore, even with thousands of research publication, it can be seen that effective security standardization is far from reality in true sense.

Table 2: Review of Credit Based Schemes.

Security Scheme	Technique	Advantage	Limitations
Secure Incentive Protocol (SIP) (Zhang *et al*, 2004)	Uses "credits" as the incentives to stimulate packet forwarding	-SIP is routing independent in the sense that it could coexist with any on demand unicast routing protocol such as DSR and AODV. -SIP is session based rather than packet based. Security module is tamper proof and hence unauthorized access is not allowed	-It needs every node to possess the hardware module and SIP is implemented in the hardware module. -Hardware module will not be available in the already existing mobile nodes
Stimulating Cooperation in Self Organizing MANETS (Mahmoud *et al*, 2011)	Uses a tamper resistant hardware module called "security module" that protects illegal manipulations	Emphasizes that the misbehavior is not beneficial and thus should occur rarely	The availability of hardware module is not guaranteed.
Sprite (Zhong *et al*, 2003)	Provide incentive to mobile nodes to cooperate using game theory	System motivates each node to report its behavior honestly, even when a collection of the selfish nodes collude	Credit Clearance Service is assumed to be reachable through the use of Internet
N-ACK(Balakrishnan *et al*, 2005)	Isolates misbehaving nodes in a MANET. If the number of times a node is adjudged as a potential misbehaving node exceeds the threshold, then the node is flagged as misbehaving.	Belief dissemination, i.e. neighboring nodes are notified about the existence of misbehaving node in their vicinity.	Results Completely depend on assumption of threshold value.
Collective Network Arbitration Protocol (CNAP) (Usha *et al*, 2010)	Sets a counter point for each node in its neighborhood list and evaluates vulnerability based on a threshold	Highly resilient against any attacks on MAC misbehavior	Results completely depend on assumption of threshold value. Not evaluated for other types of attacks
Contribution time-based Selfish Node Detection (Bakar *et al*,	each monitoring node operates in promiscuous mode and would monitor both	-Scheme performs well to detect selfish nodes -It eliminates most trust	Effect of data packet rate to the detection mechanism is not evaluated

2010)	data and control packets that are sent around within its receiving range	management complexity and avoids any false accusation and false praise attacks.	

The elaborated and extensive study of the prime categories of security measures in safeguarding the communication system in MANET is discussed and tabulated above. The prime goal of all the above mentioned security techniques is to guarantee the privacy, confidentiality, integrity, availability in the MANET system with the ability to identify precise attack patterns without false positives. It has been observed in this study is that the previously presented techniques identify and circumvent the malicious nodes in the MANET system protecting the secure channel of communication among the genuine nodes. One of the most challenging issues explored in this study is that none of the discussed protocols are either experimented or evaluated for multiple dimensionality of attack scenario in MANET. For this purpose, the research finding of the previous study just limits the efficiency of their accomplished results, considering their experimental test bed only. Hence, it is very difficult to standardize either of the security protocols in MANET, for which reason, it is almost a challenging task to propose a security protocols or techniques that has a wide range of threat mitigation capabilities in MANET considering all the quality of service parameters like packet delivery ratio, inter-arrival time of packet, latency, residual energy of a node etc.

Table 3: Review of Reputation based Schemes.

Security Scheme	Technique	Advantage	Limitations
Watch Dog and Path Rater (Abbas *et al*, 2010)	-Watchdog identifies the misbehaving node by monitoring the nearby nodes whether they forward the packets of other nodes in the network or not. -Path rater defines the best route by avoiding the misbehaving nodes.	-Improved the throughput of the network along with security. -Targeted for securing large scale MANETs	The approach does not isolate the misbehaving nodes; they still utilize the network services, i.e. the nodes are not punished for misbehaving
The 2ACK Scheme (Balakrishnan *et al*, 2005)	Detects misbehavior through the use of a new type of acknowledgment packet, termed 2ACK	Efficient for large scale MANETs with heavy traffic load	In order to reduce the additional routing overhead, only a fraction of the received data packets are acknowledged.
A Reputation-Based Mechanisms to enforce Cooperation in MANET (Anitha *et al*, 2013):	-Detects selfish nodes using three modules- i) Checking System, ii) Reputation System and iii) Priority processing System.	-Prioritizes the packet received from node based on their reputation -Selfish nodes are punished by the receiving services	Not evaluated for wide range of attacks.
Collaborative Reputation (CORE) (Pietro *et al*, 2002)	-Each network entity keeps track of other entities using collaboration. -Reputation is evaluated based on various types of information on each entity's rate of collaboration	-The source does not need to know how many nuglets need to be loaded into the packet	-Performances are not evaluated with respect to node mobility and node density -Since the packet generation is not charged, malicious flooding of the network cannot be prevented.
Cooperation of Nodes, Fairness in Dynamic Ad-hoc Networks (CONFIDANT) (Buchegger *et al*, 2002)	Perform four interdependent modules (a) monitor, (b) reputation system, (c) path manager, (d) trust manager.	Protocol is scalable in terms of the total number of nodes in a network and performs well even with a fraction of malicious nodes as high as 60%.	Behavior of the protocol over time, the performance converges or not, is not considered.

Conclusion:

This paper reviews some of the standard security techniques which are frequently adopted in majority of the current research work. The paper has discussed the security techniques from the viewpoint of its usage as in cryptography, by trusted third party, by intrusion detection system and various other methods. It can be realized that majority of the past research work has stressed on presenting a robust security techniques that mitigate the potential threats in routing procedure or else any parameters that clearly has potential impact on node mis-behaviour. Moreover, an archival of the topic is found to be flooded with wide adoption of cryptographic techniques as security measure, which is always accompanied by security loopholes. Observing the outcomes of above studies discussed in this paper exhibit that majority of the techniques more or less concentrate on malicious node without trying to understand the underlying pattern of malicious node. We strongly advocate that identification of malicious node, erroneous node, and selfish node is one of the most challenging tasks, where majority of the potential capabilities of discussed IDS system bows down. A malicious node may exhibit an abnormal behaviour even in its mobility also, which has not been considered in any test bed of the security techniques discussed in this paper.

REFERENCES

Abbas, S., M. Merabti, D. Llewellyn-Jones, 2010. A Survey of Reputation Based Schemes for MANET. In The 11th Annual Conference on The Convergence of Telecommunications, Networking & Broadcasting (PGNet 2010), Liverpool, UK, pp: 21-22.

Adams, C., S. Lloyd, 1999. Understanding the Public-Key Infrastructure: Concepts, Standards and Deployment Considerations. Sams Publishing.

Adjih, C., T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, D. Raffo, 2003. Securing the OLSR protocol. In Proceedings of Med-Hoc-Net, pp: 25-27.

Anitha, D., M. Punithavalli, 2013. A Collaborative Selfish Replica with Watchdog and Pathrater in MANETS. In International Journal of Computer Science and Mobile Computing, pp: 112-119.

Balakrishnan, K., J. Deng, V.K. Varshney, 2005. TWOACK: preventing selfishness in mobile ad hoc networks. In Wireless Communications and Networking Conference, 2005 IEEE, 4: 2137-2142.

Bakar, K.A.A., J. Irvine, 2010. Contribution Time-based Selfish Nodes Detection Scheme. PGNet.

Batra, S., P. Goyal, A. Singh, 2010. A literature review of security attack in mobile ad-hoc networks. International Journal of Computer Applications, 9(11): 11-15.

Buchegger, S., J.Y. Le Boudec, 2002. Performance analysis of the CONFIDANT protocol. In Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing, pp: 226-236.

Carter, S., A. Yasinsac, 2003. Secure position aided ad hoc routing. In Proceedings of the IASTED International Conference on Communications and Computer Networks.

Chen, J., J. Wu, 2010. A Survey on Cryptography Applied to Secure Mobile Ad Hoc Networks and Wireless Sensor Networks. Handbook of Research on Developments and Trends in Wireless Sensor Networks: From Principle to Practice, IGI Global, AH ALTALHI, 5: 2414-2424.

Cordasco, J., S. Wetzel, 2008. Cryptographic versus trust-based methods for MANET routing security. Electronic Notes in Theoretical Computer Science, 197(2): 131-140.

Hoebeke, J., I. Moerman, B. Dhoedt, P. Demeester, 2004. An overview of mobile ad hoc networks: Applications and challenges. Journal-Communications Network, 3(3): 60-66.

Hu, Y.C., A. Perrig, D.B. Johnson, 2005. Ariadne: A secure on-demand routing protocol for ad hoc networks. Wireless Networks, 11(1-2): 21-38.

Jiang, N., K.A. Hua, D. Liu, 2007. A scalable and robust approach to collaboration enforcement in mobile ad-hoc networks. Journal of Communications and Networks, 9(1): 56-66.

Junhai, L., Y. Danxia, X. Liu, F. Mingyu, 2009. A survey of multicast routing protocols for mobile ad-hoc networks. Communications Surveys & Tutorials, IEEE, 11(1): 78-91.

Kadri, B., D. Moussaoui, M. Feham, 2013. A PKI over Ant Colony based Routing Algorithms for MANETs–AntPKI–. International Journal of Network Security, 15(1): 42-49.

Koshti, D., S. Kamoji, 2011. Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks. International Journal of Soft Computing and Engineering, 1(4): 190-194.

Li, X., J. Slay, S. Yu, 2005. Evaluating trust in mobile ad hoc networks. In The Workshop of International Conference on Computational Intelligence and Security.

Lu, S., L. Li, K.Y. Lam, L. Jia, 2009. SAODV: a MANET routing protocol that can withstand black hole attack. In Computational Intelligence and Security, 2009. CIS'09. International Conference on 2: 421-425.

Mahmoud, M.E., X. Shen, 2011. An integrated stimulation and punishment mechanism for thwarting packet dropping attack in multihop wireless networks. Vehicular Technology, IEEE Transactions on, 60(8): 3947-3962.

Michiardi, P., R. Molva, 2002. Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In Advanced Communications and Multimedia Security, 4(4): 107-121.

Miranda, H., L. Rodrigues, 2003. Friends and foes: Preventing selfishness in open mobile ad hoc networks. In Distributed Computing Systems Workshops, 2003. Proceedings. 23rd International Conference on pp: 440-445.

Nikhil, K., S. Agarwal, P. Sharma, 2012. Application Of Genetic Algorithm In Designing A Security Model For Mobile Adhoc Network, pp: 181-187.

Panos, C., C. Xenakis, I. Stavrakakis, 2010. A novel intrusion detection system for MANETS. In Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on pp: 1-10.

Papadimitratos, P., Z.J. Haas, 2003. Secure link state routing for mobile ad hoc networks. In Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on pp: 379-383.

Patcha, A., A. Mishra, 2003. Collaborative security architecture for black hole attack prevention in mobile ad hoc networks. In Radio and Wireless Conference, 2003. RAWCON'03. Proceedings, pp: 75-78.

Pellegrino, G., 2006. Security Analysis of MANET in NS2. In Mini Workshop on Security Framework.

Pervaiz, M.O., M. Cardei, J. Wu, 2010. Routing security in ad hoc wireless networks. In Network Security, pp: 117-142.

Saini, R., M. Khari, 2011. Defining Malicious Behavior of a Node and its Defensive Techniques in Ad Hoc Networks. International Journal of Smart Sensors and Ad Hoc Networks, 1(1): 17-20.

Sanzgiri, K., B. Dahill, B.N. Levine, C. Shields, E.M. Belding-Royer, 2002. A secure routing protocol for ad hoc networks. In Network Protocols, 2002. Proceedings. 10th IEEE International Conference on pp: 78-87.

Sharma, A.K., P.S. Parihar, 2013. An Effective DoS Prevention System to Analysis and Prediction of Network Traffic Using Support Vector Machine Learning. International Journal of Application or Innovation in Engineering & Management, 2(7): 249-256.

Singh, G.K., H.S. Bindra, A.L. Sangal, 2011. Performance Analysis of DSR, AODV Routing Protocols based on Wormhole Attack in Mobile Ad-hoc Network. International Journal of Computer Applications, 26(5): 38-41.

Striki, M., J.S. Baras, K. Manousakis, 2008. New Algorithms for the efficient design of topology-oriented Key Agreement Protocols in Multi-hop Ad Hoc Networks. In Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops, 2008. WiOPT 2008. 6th International Symposium on pp: 384-393.

Usha, S., S. Radha, 2010. A collective network arbitration protocol to detect MAC misbehavior in MANETS. In Wireless Communication and Sensor Computing, 2010. ICWCSC 2010. International Conference on pp: 1-5.

Visalakshi, P., S. Anjugam, Security issues and vulnerabilities in Mobile Ad hoc Networks (MANET)-A Survey. nternational Journal of Computational Engineering Research, pp: 189-194.

Vishwanath, B.S., H.K. Naidu, K. Thanushkodi, M.S. Pandey, G. Vasanth, 2010. The novel application of artificial neural networks for a reliable secure wireless multicast routing in mobile ad-hock networks. In Proceedings of the ACM 12th international conference on Networking, VLSI and signal processing, pp: 54-62.

Wang, K., M. Wu, 2012. Nash Equilibrium of Node Cooperation Based on Metamodel for MANETs. Journal of Information Science and Engineering, 28(2): 317-333.

William, S., W. Stallings, 2006. Cryptography and Network Security, 4/E. Pearson Education India.

Wu, B., J. Chen, J. Wu, M. Cardei, 2007. A survey of attacks and countermeasures in mobile ad hoc networks. In Wireless Network Security, pp: 103-135.

Yoo, Y., D.P. Agrawal, 2006. Why does it pay to be selfish in a MANET?. Wireless Communications, IEEE, 13(6): 87-97.

Younis, M.F., K. Ghumman, M. Eltoweissy, 2006. Location-aware combinatorial key management scheme for clustered sensor networks. Parallel and Distributed Systems, IEEE Transactions on, 17(8): 865-882.

Zapata, M.G., 2002. Secure ad hoc on-demand distance vector routing. ACM SIGMOBILE Mobile Computing and Communications Review, 6(3): 106-107.

Zhang, C., R. Lu, X. Lin, P.H. Ho, X. Shen, 2008. An efficient identity-based batch verification scheme for vehicular sensor networks. In INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, pp: 246-250.

Zhang, Y., W. Liu, W. Lou, Y. Fang, 2006. Securing mobile ad hoc networks with certificateless public keys. Dependable and Secure Computing, IEEE Transactions on, 3(4): 386-399.

Zhang, Y., W. Lou, Y. Fang, 2004. SIP: A secure incentive protocol against selfishness in mobile ad hoc networks. In Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE, 3: 1679-1684.

Zhong, S., J. Chen, Y.R. Yang, 2003. Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks. In INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, 3: 1987-1997.

Zhu, S., S. Setia, S. Jajodia, 2006. LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. ACM Transactions on Sensor Networks (TOSN), 2(4): 500-528.

Zhu, S., S. Xu, S. Setia, S. Jajodia, 2003. LHAP: a lightweight hop-by-hop authentication protocol for ad-hoc networks. In Distributed Computing Systems Workshops, 2003. Proceedings. 23rd International Conference, pp: 749-755.