Volume 4, Issue 12, December 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey on Malicious Node Detection in MANET

Tariq Siddiqui
M.Tech Scholer CSE Dept
India

Tanveer Farooqui
A.P. CSE Dept
India

Abstract— In an Ad-hoc network is a collection of mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administer. Because of limited communication range among mobile nodes in ad-hoc network, several network hopes may be needed to deliver a packet from one node to another node in the wireless network. In such a network each node acts as an end system as well as a relay node (or router). Most of the routing algorithms designed for MANET such as AODV and DSR are based on the assumption that every node forwards every packet. But in practice some of the nodes may act as the selfish nodes. These nodes use the network and its services but they do not cooperate with other nodes. Such selfish nodes do not consume any energy such as CPU power, battery and also bandwidth for retransmitting the data of other nodes and they reserve them only for themselves. The original AODV and DSR routing algorithms can be modified to detect such selfish nodes. In this paper, we survey innovated techniques as well as proposed techniques to detect Selfish Nodes for MANET. Finally we provide some directions for further research.

Keywords— AD-HOC network, Attacks, Cooperative System in MANET, Misbehaving Nodes, Mobile Ad-hoc Network (MANET, Selfish Nodes.

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a self-configuring communications less network of mobile devices connected by wireless links. Ad-hoc is Latin word which means "for this purpose". It is the dynamic set of nodes where nodes may be any machine which able to send data or share data with all other machine. MANETs are a group of wireless ad-hoc system that generally has a routable networking atmosphere on top of a Link Layer ad hoc network. A MANET is an independent collection of movable users that exchange data over reasonably MANET increasing interactions between communication and computing, which is changing information access from "anytime anywhere" into "all the time, everywhere." At present, a large variety of networks exists, ranging from the well-known infrastructure of cellular networks to non-infrastructure wireless ad-hoc networks. Ad-hoc networks are suited for use in situations where an infrastructure is unavailable or to deploy one is not cost effective. MANETs have been broadly used in a range of military situation, such as defence force switch over information on the field, investigate teams direct in combat investigate and save hard work, and real-time enemy uncovering in the order of a troop location. In traditional networks, MANETs are more liable to cruel attacks and accidental breakdown due to their exclusive features such as constrained node energy, error-prone communication media, and dynamic network topology. Therefore, security is a very important for MANETs.

A mobile ad hoc network (MANET) is an infrastructure less network of mobile devices. In MANET mobile devices communicate on network path for routing messages from one system to a different. In MANET all devices are liberal to move in any direction, and therefore change its links to other devices frequently. Every device should send traffic unrelated to its own use, and want to be a router. The main challenge in building a MANET is equipping every device to unendingly maintain the data needed to properly route traffic. These MANETs may operate by themselves or could also be connected to the larger Internet. MANETs are a form of Wireless ad hoc network that typically includes a routable networking environment on top of a Link Layer ad hoc network. Lots of analysis has been applied in comparing MANET protocols using completely different parameters. These are focused on rising performance of MANET networks to consume energy with efficiency and routing more efficient. In ad hoc networks, nodes aren't familiar with the topology of their networks. Instead, they need to find it: a brand new node announces its presence listens for announcements broadcast by its neighbours. Every node learns concerning different close nodes and however to reach them, and make an announcement that it can also reach them. In MANETs, the nodes are mobile and battery operated. As the nodes have limited battery resources and multi hop routes are used over a changing network environment due to node mobility, it requires energy efficient routing protocols to limit the power consumption, prolong the battery life and to improve th e robustness of the system [1].

Node misbehaviour is such a category of security threat for Mobile Ad hoc Networks (MANETs). In general, misbehaviour can be conducted at every layer in MANETs, such as malicious flooding of the Request-To-Send (RTS) frames in the MAC layer, dropping, modification, and misroute to the packets in the network layer, and deliberate propagation of fake observations regarding the behaviours of other nodes in the application layer. Moreover, node misbehaviour may range from lack of cooperation to active attacks aiming at Denial-of-Service (DoS) and subversion of

traffic. For example, because of the limited resources (such as battery power and bandwidth, etc) that each node can possibly possess, a selfish node may choose not to cooperate with other nodes so as to preserve its own resources [2]. In other words, when a selfish node is requested to forward some data packets for other nodes, it might drop a part or all of the incoming packets. By this means, it can save the battery power and transmit some extra packets for the sake of itself. On the other hand, some malicious nodes aim to disturb the network services, and they may intentionally drop, modify or misroute packets while it is not a priority for them to save battery lives [3]. Regardless of the intents by which the node misbehaviour are induced, they are obviously harmful to a currently healthy MANET.

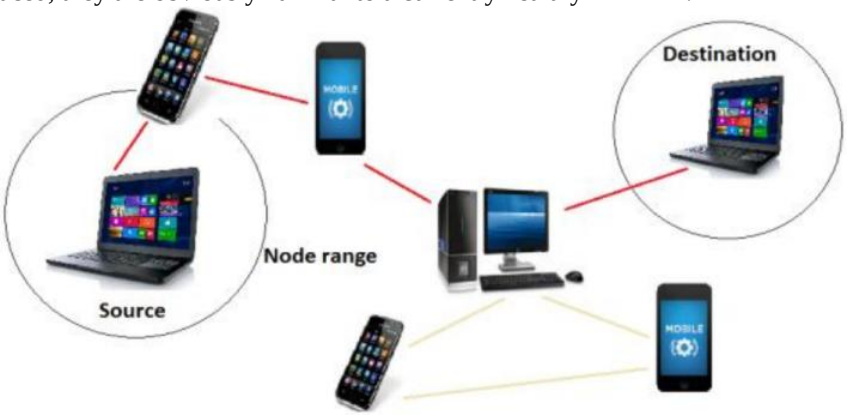

Fig 1. MANET Architecture

To address the security vulnerabilities caused by various node misbehaviour in Mobile Ad hoc Networks (MANETs), numerous security solutions have been proposed to detect and mitigate those misbehaviour from distinctive perspectives, such as the mechanisms discussed accordingly in [4], [5], and [6]. Because it is quite beneficial to assess a node's behaviours and determine if it is trustworthy in terms of how cooperative it is, trust management mechanism has become a power tool to cope with node misbehaviours. A variety of trust management mechanisms have been studied during the past decades, such as the mechanisms discussed in [6], [7], and [8]. Most of these trust management mechanisms model the trust of a node in one dimension, i.e., all available evidence and observations are utilized to calculate a single, scalar trust metric for each node. However, a single trust metric may not be expressive enough to adequately describe whether a node is trustworthy or not in many complicated scenarios

II. RELATED WORK

In the past decade, many research efforts have been made to address the security needs for MANETs by means of trust management [9]. The main goal of trust management is to evaluate the actions of other nodes, and build a reputation for each node based on the node evaluation result. The reputation can then be used to determine the trustworthiness for other nodes. The trustworthiness can be utilized to make choices on which nodes to cooperate with, or even take action to punish an untrustworthy node if necessary. Trust is divided into direct trust and indirect trust [10]. Direct trust stems from the first-hand observations locally obtained by a node itself, while indirect trust refers to the second-hand observations released by other nodes. In MANETs, direct trust cannot always provide comprehensive evaluation of the target node due to exterior circumstances such as channel conditions, temporary unavailability, interference, etc. At this time, indirect trust is used to provide secondary information to help evaluate the actual trustworthiness of the target node.

In recent years, there has been significant research interest in the topics of misbehaviour detection as well as trust management for ad hoc networks. Hence, the related work for these two research topics will be presented separately in this section.

A. Misbehaviour Detection for Ad hoc Networks

When it comes to the discussion of misbehaviour detection, we should first clearly understand the term misbehaviour itself. Note that the term misbehaviour generally refers to abnormal behaviour that deviates from the set of behaviours that each node is supposed to conduct in MANETs [13]. According to [14], there are four types of misbehaviours in ad hoc networks, namely failed node behaviours, badly failed node behaviours, selfish attacks, and malicious attacks. These four types of node misbehaviours are classified with respect to the node's intent and action. More specifically, selfish attacks are intentional passive misbehaviours, where nodes choose not to fully participate in the packet forwarding functionality to conserve their resources, such as battery power; malicious attacks are intentional active misbehaviours, where the malicious node aims to purposely interrupt network operations. The existence of selfishness and malicious behaviours has remarkably motivated research in the area of misbehaviour detection for mobile ad hoc networks. Intrusion Detection System (IDS) is normally regarded as an important solution for detecting various node misbehaviours in MANETs. Several approaches have been proposed to build IDS probes on each individual peer due to the lack of a fixed infrastructure, such as [11, 15, 16]. In these approaches, there is one IDS probe installed on each node, and each IDS probe is assumed to be always monitoring the network traffic, which is obviously not energy efficient given the limited battery power that each node has in MANETs. In contrast, Huang et al. [12] proposed a cooperative intrusion detection framework in which clusters are formed and the nodes in each cluster will fulfil the intrusion detection task in turn.

B. Trust Establishment and Management in Ad hoc Networks

The main purpose of trust management is to assess various behaviours of other nodes and build a reputation for each node based on the behaviour assessment. The reputation can be utilized to decide trustworthiness for other nodes, make choices on which nodes to cooperate with, and even take action to punish an untrustworthy node if necessary.

In general, the trust management system usually relies on two sorts of observations to evaluate the node behaviours. The first kind of observation is named as first-hand observation, or in other words, direct observation [17]. First-hand observation is the observation that is directly made by the node itself, and the first-hand observation can be collected either passively or actively. If a node promiscuously observes its neighbours' actions, the local information is collected passively.

In contrast, the reputation management system can also rely on some explicit evidences to assess the neighbour behaviours, such as an acknowledge packet during the route discovery process. The other kind of observation is called second-hand observation or indirect observation. Second-hand observation is generally obtained by exchanging first-hand observations with other nodes in the network. The main disadvantages of second-hand observations are related to overhead, false report and collusion [18], [19].

C. Routing Protocols

Routing Protocol is used to find valid routes between communicating nodes. They do not use any access points to connect to other nodes. It must be able to handle high mobility of the nodes. Routing protocols can be mainly classified into 3 categories:

1) Table Driven (Proactive) Protocol

Each node inside the network has routing table for the broadcast of the information packets and want to establish connection to completely different nodes inside the network. These nodes record for all the presented destinations and number of hops required to reach every destination inside the routing table. The routing entry is labelled with a sequence number that's formed by the destination node. To retain the steadiness, each station broadcasts and updates its routing table time to time. Every node contains the following information:

- How many hops are required to arrive that exact destination node.
- Generation of new sequence number marked by the destination.
- The destination address.

The proactive protocols are appropriate for fewer numbers of nodes in networks, because they need to update node entries for each and every node within the routing table of each node. It results a lot of Routing overhead problem. There is consumption of more bandwidth in routing table. Example: DSDV (Destination-Sequenced Distance-Vector), CGSR (Cluster gateway Switch Routing), WRP (Wireless Routing Protocol).

2) On-Demand (Reactive) Protocol

On-demand protocols, computes the routes and maintain routing information only if it is required and nodes establish routes only when required by the source. Route maintenance procedure helps in maintaining route information from source to destination. The routes are kept in routing memory of n odes as long as required. The route maintenance procedure was designed to overcome the wasted effort in maintaining unused routes. Reactive routing protocols sends out unnecessary messages to find the routes, they are not optimal in terms of bandwidth utilization, but they scale well in the frequency of topology change. Example: Ad Hoc On -Demand Distance Vector (AODV), Dynamic source routing (DSR), Location-aided routing (LAR).

3) Hybrid Protocol

Hybrid routing protocols include the benefits of each proactive and reactive protocols. This protocol is classified as a flat protocol due to overlapping of zones. As a result network congestion is sometimes reduced and best routes are usually detected. Each MN defines 2 zones: the within zone and also the outside zone. The hybrid protocols act as proactive protocols in the within zone and reactive protocols within the outside zone.

Packets are broadcasted periodically in the within zone to create a routing table for all MNs in the within zone. When a node desires to send information to a destination node that resides within the outside zone, it uses a reactive protocol. Thus, a route discovery phase is invoked to determine the route to the destination MN. Example: ZRP (Zone Routing Protocol).

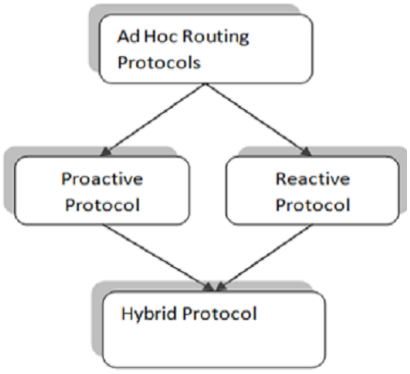

Fig. 2. Routing Protocols

D. Types of Attack in MANET

Securing wireless ad hoc networks is a massive challenge. Before offering security in MANET or any ad hoc network, it is essential to understand probable kind of attacks. Ad hoc networks attack can be classified as inactive or active [20]. A passive attack obtains data exchanged in the network without disrupting the operation of the communications, while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a MANET. The attacks can also be classified into 2 categories, namely external attacks and internal attacks, according the domain of the attacks. External attacks are carried out by nodes that don't belong to the domain of the network. Internal attacks are from compromised nodes that are actually part of the network. Internal attacks are more severe because an insider attack knows valuable and secret information, and possesses privileged access rights.

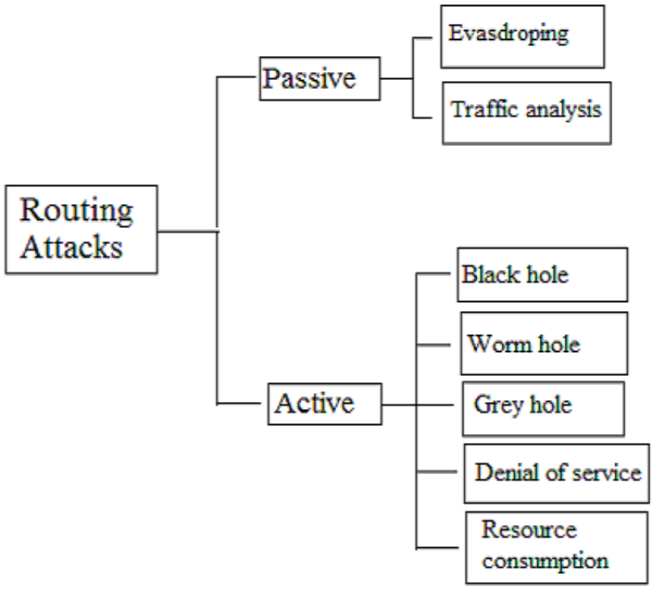

Fig. 3. Possible Security Attacks in MANET.

Active attack can be defined as "the attacker or fraud modify or alter the knowledge which may be shared among the nodes in the networks". The active attacks are usually launched by compromised nodes or malicious nodes. Malicious nodes change the routing data by advertising itself as having shortest path to the destination [20]. In MANET an attacker hurt the network performance by inappropriately modifying the routing message, injecting mistaken messages, or pretending a certified Mobile Node to confuse the traditional network.

Black hole attack is a sort of attacks, malicious node claims having an optimum route to the node whose packets it desires to intercept. On receiving the request the malicious node sends a fake reply with very short route [20]. In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it. A malicious node sends fake routing information, claiming that it has an optimum route and causes alternative good nodes to route information packets through the malicious one. A malicious node drops all packets that it receives rather than normally forwarding those packets.

In Wormhole Attack, a wrongdoer receives packets at one point within the network, tunnels them to a different point in the network, and then replays them into the network from that point. Routing can be discontinuous once routing control message are tunnelled. This tunnel between 2 colluding attacks is known as a wormhole.

Denial of Service aims to attack the availability of a node or the entire network. If the attack is successful the services will not be available. The attacker usually uses radio signal jamming and the battery exhaustion method. Gray-hole attack is also known as routing misbehaviour attack which leads to dropping of messages. Gray hole attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability.

In Resource Consumption Attack an attacker tries to consume or waste away resources of other nodes present in the network. The resources that are targeted are battery power, bandwidth, and computational power, which are only limitedly available in ad hoc wireless networks. The attacks could be in the form of unnecessary requests for routes, very frequent generation of beacon packets, or forwarding of stale packets to nodes. Using up the battery power of another node by keeping that node always busy by continuously pumping packets to that node is known as a sleep deprivation attack. Attacks under this category, are directly affects the self-performance of nodes and does not interfere with the operation of the network [20]. It may include two important factors.

- Saving of battery power.
- Obtaining unfair share of bandwidth.

Modification, a malicious node modifies message throughout the transmission between the communication nodes, attackers modify packets and disrupt the overall communication between network nodes [20]. As an example, an attacker can deliberately shorten or lengthen the node list within the routing packet, lengthen the messages.

IP spoofing, malicious node sends a internet protocol packet containing its own Mac address and a victim's ip address, thereby usurping the IP-to-MAC address binding of the victim from the alternative neighbour's Address Resolution Protocol (ARP) cache.

In Tunnelling attack, a malicious node creates a very different kind of routing disturbance, known as tunnelling attack [21], and by using a pair of malicious nodes connected along via a private network connection [21]. Every packet received node A are forwarded to node B through their personal connection. This attack can most likely disturb routing by short circuiting the same old flow of routing packets. It implies that that if approved sender sends packets; it can be catched by personal network of trespasser being receiver so intruder send smashed packets to approved receiver.

Passive attack: it is an attack where an unofficial wrongdoer monitors or listens to the communication among two parties. It means that wrongdoer or intruder never send any corrupted message in a MANET network. A wrongdoer may inactively hear the network traffic to gather valuable data, like network connectivity, node location, traffic distribution, and so on. The main goal of passive attacks is to come up with threat against the network privacy [20]. Compared with active attacks, passive attacks are really powerful to prevent and find because the intruders aren't concerned in any modification of transmitted message or disruption of the network activity. Relying on dissimilar actions taken by an wrongdoer, passive attacks can be additional separated into following subcategories.

Eavesdropping: An assaulter will get direct data of the network by intercepting transmitted data packets. Passive eavesdropping may be prohibited by a range of encryption schemes and defensive the privacy of the data transmission, thus assaulter cannot acknowledge the encrypted data and it's key.

Traffic analysis attacks: AN attack might dig out valuable information from the distinctiveness of the transmission like node identity, the number of transmitted packets, time required to send one bit or a packet and also the frequency of data transmission. The extracted information may enable the wrongdoer to do a n auxiliary analysis and decipher some sensitive information [20]. Traffic analysis in ad hoc networks might reveal following sort of info.

- Location of nodes.
- Network topology used for communication.
- Roles played by nodes.
- Available source and destination nodes.

III. TECHNIQUES IN MALICIOUS NODE DETECTION

Due to its dynamic nature and mobility of nodes, mobile adhoc networks are more vulnerable to security attack than conventional wired and wireless networks. One of the principal routing protocols AODV used in MANETs. The security of AODV protocol is influence by malicious node attack. In this attack, a malicious node injects a faked route reply claiming to have the shortest and freshest route to the destination. However, when the data packets arrive, the malicious node discards them. To preventing malicious node attack, paper [22] presents PPN (Prime Product Number) scheme for detection and removal of malicious node.

The paper [23] proposes to use a statistical inference technique, namely, belief propagation (BP), to estimate the probability of peers being malicious. The detection algorithm is run by a set of trusted monitor nodes that receives notification messages (checks) from peers whenever they obtain a chunk of data; these checks contain the list of the chunk up loaders and a flag to mark the chunk as polluted or clean. Peers are able to detect if the received chunk is polluted or not but, since multiparty download is employed, they are not capable to identify the source(s) of bogus blocks.

To find out malicious nodes among a WSN with mass sensor nodes, this paper [24] presents a malicious detection method based on multi-variate classification. Given the types of a few sensor nodes, it extracts sensor nodes' preferences related with the known types of malicious node, establishes the sample space of all sensor nodes that participate in network activities. Then, according to the study on the type-known sensor nodes' samples based on the multivariate classification algorithm, a classifier is generated, and all of the unknown-type sensor nodes are classified.

the sensitivity of Wireless Sensor Networks makes them prone to attacks which lead to extraction or damage of data or information that flows between distinct nodes. The main objective of paper [25] is to construct an effective sensor security detection system which is adaptive to the behavioural changes of the nodes and the data flowing between various sensor nodes and hence detect the malicious node in our environment based on its skeptical behaviour.

Preventing or detecting malicious nodes launching grayhole or collaborative blackhole attacks is a challenge. This paper [26] attempts to resolve this issue by designing a dynamic source routing (DSR)-based routing mechanism, which is referred to as the cooperative bait detection scheme (CBDS), that integrates the advantages of both proactive and reactive defence architectures. Our CBDS method implements a reverse tracing technique to help in achieving the stated goal. Simulation results are provided, showing that in the presence of malicious-node attacks, the CBDS outperforms the DSR, 2ACK, and best-effort fault-tolerant routing (BFTR) protocols (chosen as benchmarks) in terms of packet delivery ratio and routing overhead (chosen as performance metrics).

TABLE I VARIOUS TECHNIQUE COMPARISON

Author	Year	Model	Processing techniques	Application
Gambhir S. [29]	2013	PPN (Prime Product Number) scheme	Adhoc On-demand Distance Vector to make path during path discovery	for detection and removal of malicious node.
Gaeta R.	2013	use a statistical	set of trusted monitor nodes that	to estimate the probability of

[30]		inference technique	receives notification messages	peers being malicious.
Hongjun Dai [31]	2012	malicious detection method	method based on multi-variate classification	To find out malicious nodes among a WSN
Singh, M. [32]	2012	construct an effective sensor security detection system	adaptive to the behavioural changes of the nodes	hence detect the malicious node in WSN environment
Chang, J.-M [33]	2014	cooperative bait detection scheme (CBDS) method	a reverse tracing technique	Preventing or detecting malicious nodes launching grayhole or collaborative blackhole attacks
Narayanan, S.S. [34]	2013	A defence mechanism	MAC address of the destination to validate each node	providing a direct negotiation for secure route
Amaresh, M. [35]	2013	the combination of trust and energy value	routing protocol called Energy and Trust Based AODV routing protocol	to establish a most trusted routes

Ad hoc on-demand distance vector routing (AODV) is a very popular routing protocol. However, it is vulnerable to the well-known black hole attack, where a malicious node falsely advertises good paths to a destination node during the route discovery process. In paper [27], a defence mechanism is presented against these black hole attacks in a MANET. This method makes use of the MAC address of the destination to validate each node in its path thereby providing a direct negotiation for secure route.

Paper [28] Proposed model uses the combination of trust and energy value based routing protocol called Energy and Trust Based AODV routing protocol (ET-AODV) to establish a most trusted routes by providing modification to AODV protocol. In proposed technique each node estimates its neighbour's trust value and energy value that is one node has for another node during communication dynamically. Adding trust value and energy value new root value is calculated and maintained in every neighbour table. Using root value trusted routes are established by two methods that are single value routing and multiple value routing and isolate the malicious nodes from the network. This technique only considers the black hole attack which can easily interrupt the communication path.

IV. CONCLUSION

As the use of Mobile Ad hoc Networks (MANETs) has increased, the MANETs security has become more important accordingly. No doubt the IDS are here to keep our systems safe; however, future systems will definitely take a different form from our modern-day versions. In this survey research, we have discussed Classification of selfish nodes detection techniques, Various Intrusion detection techniques, Various Innovated selfish node detection techniques and Various Proposed selfish node detection techniques for mobile ad hoc networks.

As the survey is conducted in literature survey, this work comes through the various techniques to detect various attacks. Thus there are vast numbers of techniques to detect attacks on MANET security. Intrusion detection techniques also should be integrated with existing MANET application. This requires an understanding of deployed applications and related attacks in using suitable intrusion detection mechanisms. An intrusion detection system aims to detect attacks on mobile nodes or intrusions into the networks. However, attackers may try to attack the IDS systems itself. In our future we plan to propose a new efficient technique to detect selfish nodes in MANET

REFERENCES

[1] Varsha Patidar, Rakesh Verma "Risk Mitigation of Black Hole Attack for Aodv Routing Protocol", IOSR Journal of Computer Engineering (IOSRJCE) Volume 3, Issue 3 (July-Aug. 2012), PP 12-15.

[2] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Commu-nications and Multimedia Security. Deventer, The Netherlands, The Netherlands: Kluwer, B.V., 2002, pp. 107–121.

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

[4] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking. New York, NY, USA: ACM, 2000, pp. 275–283.

[5] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," inMobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking. New York, NY, USA: ACM, 2000, pp. 255–265.

[6] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the confidant protocol," in MobiHoc '02: Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing. New York, NY, USA: ACM, 2002, pp. 226–236.

[7] G. Theodorakopoulos and J. S. Baras, "Trust evaluation in ad-hoc networks," in WiSe '04: Proceedings of the 3rd ACM workshop on Wireless security. New York, NY, USA: ACM, 2004, pp. 1–10.

[8] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, "Robust cooperative trust establishment for manets," inSASN '06: Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks. New York, NY, USA: ACM, 2006, pp. 23–34.

[9] J. Cho, A. Swami, and I. Chen, "A survey on trust management for mobile ad hoc networks," Communications Surveys Tutorials, IEEE, vol. PP, no. 99, pp. 1 –22, 2010.

[10] G. Theodorakopoulos and J. S. Baras, "Trust evaluation in ad-hoc networks," in WiSe '04: Proceedings of the 3rd ACM workshop on Wireless security. New York, NY, USA: ACM, 2004, pp. 1–10.

[11] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking. New York, NY, USA: ACM, 2000, pp. 275–283.

[12] Y.-A. Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks," in SASN '03: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks. New York, NY, USA: ACM, 2003, pp. 135–147.

[13] S. Buchegger and J.-Y. Le Boudee, "Self-policing mobile ad hoc networks by reputation systems," IEEE Communications Magazine, vol. 43, no. 7, pp. 101–107, July 2005.

[14] P.-W. Yau and C. J. Mitchell, "Security vulnerabilities in ad hoc networks," in Proceedings of the 7th International Symposium on Communication Theory and Applications, 2003, pp. 99–104.

[15] H. Deng, Q.-A. Zeng, and D. Agrawal, "Svm-based intrusion detection system for wireless ad hoc networks," in Proceedings of 2003 IEEE 58th Vehicular Technology Conference, 2003. VTC 2003-Fall., vol. 3, Oct. 2003, pp. 2147–2151.

[16] C.-Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt, "A specification-based intrusion detection system for aodv," in SASN '03: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks. New York, NY, USA: ACM, 2003, pp. 125–134.

[17] S. Buchegger and J.-Y. L. Boudec, "A robust reputation system for mobile ad-hoc networks," in Proceedings of P2PEcon, 2003.

[18] Q. He, D. Wu, and P. Khosla, "Sori: a secure and objective reputationbased incentive scheme for ad-hoc networks," in Proceedings of 2004 IEEE Wireless Communications and Networking Conference, WCNC '04., vol. 2, March 2004, pp. 825–830 Vol.2.

[19] S. Buchegger and J.-Y. L. Boudec, "The effect of rumor spreading in reputation systems for mobile ad-hoc networks," in Proceedings of WiOpt 2003: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, 2003.

[20] Jaya Jacob, V.Seethalakshmi. "Performance Analysis and Enhancement of Routing Protocol in MANET", International Journal of Modern Engineering Research (IJMER) ,Vol.2, Issue.2, Mar-Apr 2012 pp-323-328.

[21] Sandeep Lalasaheb Dhende, Prof. D. M. Bhalerao "Detection/Removal of Black Hole Attack in Mobile Ad-Hoc Networks" International Journal of Advanced Research in Computer Science and Electronics Engineering Volume 1, Issue 6, August 2012.

[22] Gambhir, S. ; Sharma, S., "PPN: Prime product number based malicious node detection scheme for MANETs", IEEE 3rd International on Advance Computing Conference (IACC), Page(s): 335 – 340, IEEE, 2013.

[23] Gaeta, R. ; Grangetto, M., "Identification of Malicious Nodes in Peer-to-Peer Streaming: A Belief Propagation-Based Technique", IEEE Transactions on Parallel and Distributed Systems, Volume: 24, Issue: 10, Page(s): 1994-2003, IEEE, 2013.

[24] Hongjun Dai ; Huabo Liu ; Zhiping Jia ; Tianzhou Chen , "A Multivariate Classification Algorithm for Malicious Node Detection in Large-Scale WSNs", International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Page(s): 239 - 245, IEEE, 2012.

[25] Singh, M. ; Mehta, G. ; Vaid, C. ; Oberoi, P., "Detection of Malicious Node in Wireless Sensor Network Based on Data Mining", International Conference on Computing Sciences (ICCS), Page(s): 291- 294, IEEE, 2012.

[26] Chang, J.-M. ; Tsou, P.-C. ; Woungang, I. ; Chao, H.-C. ; Lai, C.-F., "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach", IEEE Systems Journal, , Volume: PP, Issue: 99, Page(s): 1- 11, IEEE, 2014.

[27] Narayanan, S.S. ; Radhakrishnan, S., "Secure AODV to combat black hole attack in MANET", International Conference on Recent Trends in Information Technology (ICRTIT), Page(s): 447-452,IEEE, 2013.

[28] Amaresh, M. ; Usha, G., "Efficient malicious detection for AODV in mobile ad-hoc network", International Conference on Recent Trends in Information Technology (ICRTIT), Page(s): 263- 269, IEEE, 2013.

