International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.6, No.7, July 2017 DOI:10.15693/ijaist/2017.v6i7.25-30

A Survey on Performance Analysis of ManetsUnder Security Attacks

P.V.S. Siva Prasad,
M.Tech, Associate Professor, Research Scholar,
Rayalaseema University, Kurnool, Andhra Pradesh.
sivaprasadpvs@gmail.com

Dr.S. Krishna Mohan Rao,
M.Tech, PhD, Principal, Gandhi Institute for Technology (GIFT), Bhubaneswar.
princispal@gift.edu.in

Abstract—the shift to wireless network from wired network has emerged to be a worldwide trend in the lastcouple of decades. The mobility and scalability rendered by wireless network have made it feasible in several applications. Among all of the current wireless networks, Mobile Ad hoc NETwork (MANET) is one among the most essential and distinct applications. Contrary to the conventional network architecture, MANET does not need a predefined network infrastructure; each single node functions both as a transmitter and a receiver. Nodes communicate directly with one another when both of themlieinside the same range of communication. Else, they depend on their neighbors for relaying messages.Owing to the dynamic behavior of mobile Ad-HOCnetwork it is more susceptible to intrusions.Hence, security is a more importantchallengecompared to infrastructure-based wireless networks. In MANETs, it is hard to find thevicious hosts since the networktopologyvaries dynamically. A malicious intruder can easily intervene a route for which it is one among the forming nodes existing in the communication path. In the earlier works, there are various proposals to identify such dangerousattack like black hole, gray hole, worm hole, collaborative black hole, Byzantine attacks, Sybil and sink hole. The available research techniques are explained with their pros and cons, such that the research works carried out in future can focus them more.

Keywords - MANET, Routing, Collaborative Attacks and Active Attacks.

I. INTRODUCTION

Mobile ad hoc networks (MANETs) are getting increasing more attention as an element of the next-generation network technologies. These networks are generallybuilt by making use of mobile and wireless hosts with minimal or no centralized control point of attachment, like a base station [1].Everynode in MANET is fitted with awireless transmitter and receiver that permits it tocommunicate with the rest of the nodes within its radio communicationrange with no fixed infrastructure. In case a node desires toa packetforwarded to a node, which lies outside its radio range, then it needs thecollaboration of other nodes present in the network.Hence, every node has to don the hat of as both a host and a router simultaneously [2].

MANET is specificallyunguardedowing to its basicfeatures, like open medium, dynamic topology, distributivecollaboration, and limited capability. Routing has avital role to play in the security aspect of the whole network.The chiefobjective of routing protocols in MANET is to reduce the delay and to increase the network throughput, network lifespan and energy efficiency [3]. Routing protocols can be divided into three: Proactive (Table-driven), Reactive (Ondemand) and Hybrid. Proactive routing protocols discover routes between each and every source- destination pair and save them in the routing table, evenwhen they are not required. Few of the proactive protocols includeDestination Sequenced Distance Vector (DSDV), WirelessRouting Algorithm (WRP), Global State Routing (GSR), etc.These protocols experience very less delay in the determination of route.Since the network is greatly dynamic, periodic update of theroutes isrequired. The routes that are notutilizedat all are alsomaintained and updated often that is again substantial wastage of resources [4].

Reactive routing protocols discover the routes to destination solelyif they are required. They are known as On-demandprotocols, since they begin the route discovery process only duringdemand. Few of the reactive protocols include Dynamic SourceRouting protocol (DSR), Ad hoc On-demand Distance Vector (AODV) protocol, Temporally Ordered Routing Algorithm (TORA), etc. There is no overhead due to periodicupdates and theirscalability ishigh. These protocols offer better route latency because of route discovery that can be surpassedby route caching. Hybrid routing protocols like Zone RoutingProtocol (ZRP) possess reactive and proactive features.

Mobile ad hoc networks are hugely vulnerable to routing threatsdue to their dynamic topology and absence of any infrastructure. The ad-hoc networks possess a dynamic topologyimplying that the nodes are characteristically mobile, such that they can join or move away from the network easily at any point of time. On the other hand, they impose several non-trivial problemswhile designing forsecurity since they are more susceptible to attacks compared to wired networks. They are divided mainly into Active Attack and Passive Attack. A passive attack would not perturb the normal function of mobile ad hoc network, when there is exchange of data from

the network. The intruders do notdirectlyharm to the network. But, they can acquireknowledge for malicious attacks in the future. The kinds of passive attacks include eavesdropping and traffic analysis [5].

In active attack, an intruder always attempts to change or incur damage to the information or normal functioning on MANET. Active attacks could be either internal or external. In the case of external attack, the attacker concentrates on the ways of causing congestion in the network. To do this, they broadcastfalsified information or bring in disturbance in the nodes from offering services. In the case of internal attacks, the attacker is required to have the normal access to take part in theactivities of the network. The active attacks include dropping, modification, and fabrication and Timing attacks. Moreover, Security attack include Wormhole attack, Blackhole attack, Grayhole attack or Selective packet drop attack, Byzantine attack, Sybil attack and Flooding attackthatcomes under the network layer attacks.

Sukla Banerjee [6] introduced a technique for discovery/elimination of collaborative black and gray-hole attack in mobile ad-hoc networks. Here, rather thantransmitting the entire data traffic at one point of time, thewhole traffic is split into few small sized blocks. This way, thecompromised nodes can be identified and eliminated during the transmission of two such blocks by guaranteeing an end-to-end verification. Source node transmits a prelude message to the destination node prior to starting to send any block, in order to signal it regarding the incoming data block. Khemariya et.al [7] explains their mechanismto be capable of safeguarding against single and cooperative black hole attacks for MANETs. It is stated that even if the node is idle,it is quite successful. Nonetheless, the approach has differentstrategies for idle and communicating nodes.

Collaborative Attacks (CA) belong to new generation attack that can be describedto be a homogeneous attack (i.e. blackhole or wormhole attack), that involves two or more number of intruding nodes; grouped under internal active attack that can be processed employing wired or wireless link and initiated by single or more than one attacker. Every individual intruder may possessspecific expertise. Variable number of attacks happens while a system is intervened by multiple attackers, but they may not be necessarily collaborated. Numerousmethodologies are studied with which few of the collaborative attacks can be oppressed with and identifying them easily isfeasible inmany attacks. But all the earlierstrategies are susceptible to an entire set of collaborative attacks.

II. LITERATURE SURVEY

Gupta et.al [8] developed a Black hole Avoidance Protocol (BAAP) thatprevents black hole attack without using any specialized hardware and relying on physical medium of wireless network. This protocol employsAdhoc on demand multipath distance vector (AOMDV). Here, in thisprotocol each node maintains the legitimate nature of their neighboring nodes to create the right path to destination node. In the discovery of path, an intermediate node will try to make a route, which does not pass through a node whose legitimacy ratio cuts across the lower threshold level. If the malicious node is not present, then this protocol needssome more time. With increase in mobility, packet loss also increases.

Hayajneh et al. [9] presented novel approach for wormhole detection known as De Worm that identifies alternative path to get around wormhole, by means of comparison of the length of theroutes to certain thresh hold. De Worm performs the checking of the length ofalternative routes between nodes, which are apartby a short distance and employs a forbidden list to prevent the neighboring nodes in the rangeof wormhole. Sender will then consider two hop neighbors to be the target, and then inform all of its neighbors to look for a path to that hop. Senderwill then consider one path, decide its length and then compare it withthe longest length. When the length is considerably low compared to thethreshold, wormhole is identified; else the process is repeated till it reaches two hop from the actuallyspecified destination.DeWorm is not related to a particular routing protocol andthis is not verified for mobile systems.

Jian-Ming Chang [10] developed a detection mechanismreferred to as the cooperative bait detection scheme (CBDS), for the detection of dangerous nodes in MANETs leading to black hole attack.In this method, the source node arbitrarilychooses the address of a neighbour nodeto be a bait address and then a bait packet (RREQ') is transmitted to attract themalicious nodes to transmit a reply RREP. As themisbehaving node doesn't cross-check its routing table, it will send a reply although the RREQ' has afake destination address. Every time the malicious node replies, it is saved in the black list and then it is identified to be a malicious node and stopped from taking part in the routing operation, Moreover, the packet delivery ratio gets checked at the destination and when it slips to a predefined threshold, then an alarm is transmitted by the destination node to the source node in order to initiate the detection mechanism once more.

Ngai et al. [11] firstsuggested a mechanism for identifying the sinkhole assaults thatincludesthe BS in the location process, conveying a hoisted correspondence cost for the pattern. The system overflows by the BS with a solicitation message that includes the IDs of the impacted hubs. The affected hubs relay an answer to the BS with a message having their IDs, ID of the jump that follows and the corresponding cost. Then data is used from the BS to design a system stream chart for identifying the sinkhole. This detection mechanism is identical to the Ad Hoc On-interest Distance Vector Protocol (AODV) and the Dynamic Source Routing (DSR) Protocol.

Kalia andMunjal [12] presented a technique thatutilizes the fuzzy based control, to identify and mitigate a kind ofattack, such as the malicious packet dropping, in wireless ad-hocnetwork. A dangerous node in a network guarantees to forward thepackets but drops or else delays them. In this method, each nodein the mobile ad-hoc network transmits the route request and thenwaits for the acknowledgment. The requesting nodeevaluatesthe behavior of unknown node employing fuzzy technique and based on the result, the node considers this node in the route of thepacket. Consequently, the states of the nodes can also be usedby the routing protocol to get through those dangerous nodes. Their technique indicates that in a dynamically varying network, the method can identify many of the malicious nodes with aconsiderably high positive rate. Moreover, the packet delivery rate in theMANET can also be incrementedin accordance.

Weerasinghe and Fu [13] developed an algorithm to detect the Collaborative Black Hole Attack. In this, the AODV routing protocol is modified slightly by having one more additional table i.e. Data Routing Infonnation (DRI) table and then verifyingemploying Further Request (FREQ) and Further Reply (FREP). In case the source node (SN) does not possess the route entry to the destination, it will propagate a RREQ (Route Request) message to find a secure route to the destination node just as in the AODV. Any node which hasgot this RREQ either provides a reply for the request or else broadcasts it again to the network based on the availability of new route to the destination. In case the destination sends a reply, all the intermediate nodes update or insert the routing entry for that destination asthe destination is always trusted. Also, the source node trusts the destination node and will begin to transmit data on the routealong which reply returns back. Moreover, the source node will update the DRI table with all the intermediate nodes located between source and the destination.

Abbas et.al [14] developed a lightweight mechanism to identify the new identities of Sybil attackers without employing central trusted third party or any additional hardware, like directional antennae or a geographical positioning system.In specific, the new mechanismuses the RSSfor the purpose of differentiating between the authorized and Sybilidentities. First, the entry and exit characteristicof authorized nodes and Sybil nodes are demonstrated. Secondly, a threshold, which differentiates between the authorized and Sybil identities on the basis of the entry and exit behavior of the nodes. Thirdly, the detectionthreshold is tuned by including the RSS data fluctuation considered. Depending on the threshold, detection mechanism is applied. The mechanism can be usedfor both scenarios of Sybil attacks, i.e., if the new identities are formed one after another or at the same time,are just as the same to the detection process.

Yu et.al developed [15] a secure routing protocol to defend againstbyzantine attacks for MANETs in hostile environments.One new algorithm identifies the internal attacks by employing both message and route redundancy during the process of route discovery. The route-discovery messages are safeguarded by means of pairwise secret keys between a source and destination and few intermediate nodes along a route created by applying public key cryptographic schemes. Also an optimal routing algorithm is combined with routing metric for the reliability and performance of the node. A node formsitsreliabilityover its neighborhood nodes depending on theobservations made on the neighbor nodes' behaviors. Both the algorithmsdesigned can be combined into the already available routing protocols for MANETs, like ad hoc on-demand distance vector routing (AODV) and dynamic source routing (DSR) to accomplish high packet delivery ratio and security.

Shakshukiet.al [16] examined a secure intrusion-detection referred to as Enhanced Adaptive ACKnowledgment (EAACK). This novel approach EAACK is developed in order to deal with threeof the six drawbacks of Watchdog mechanism, including, falsemisbehavior, restricted transmission power, and receiver collision.EAACK comprisesof three important parts, known as, ACK,secure ACK (S-ACK), and misbehavior report authentication(MRA). In this new system, it is assumed that the link between every node in the network is bidirectional. Moreover, for every communication process, both the source node and the destination node are not adversarial. Except when indicated, all the acknowledgment packets specified in this research work need to be digitally signed by its sender and thenchecked by its receiver. EAACK exhibitsgreater malicious- behavior-detection rates in somescenarioswhereas it does not impact the network performancesgreatly.

Rathiga et.al [17] developedanew hybrid black/gray hole detection approach is for the detection of both the black and gray hole attacks in Dynamic Source Routing (DSR) protocol for MANET by employing the same method. DSR protocol dynamically finds a source route across several network hops to any destination present in the MANET. In this hybrid methodology, the initialized monitor nodes gather the packet flow informationregarding the neighboring nodes. Thereafter the information distance metric is calculatedemploying which two detection thresholds are fixed. After this,the comparison of the distance metric for each of the nodes is done with the first threshold. In case the information distance metric of a node is highercompared to the first detection threshold, then the node is treated to be adversarial nodes. Else if the information distance metric of the nodes isless than the second threshold but not smaller than the first threshold, then the nodes are labelled as gray hole attackers whereas if they are higher than the second threshold, then the nodes are labelled as black hole attackers. The hybrid detection mechanismidentifies and removes the attacks in an effective manner with better throughput, packet drop rate, packet delivery ratio and routing overhead.

Gandhewar et.al [18] investigated on detectionand prevention of sinkhole attack on AODV Protocol in Mobile Adhoc. OIT chieflycomprises of four phases as Initialization Phase, Storage Phase, Investigation Phase, and Resumption Phase. This algorithm will be positioned at intermediate nodes in the network. It actuallybegins with Initialization phase, where AODV commences its route discovery phase by broadcasting RREQ to all of its neighbors for getting the needed shortest &new path to the destination, and then the next subsequent phase of algorithm begins by saving therequired information of every RREQ in route the routing table that chiefly includes the sequence number, hop count & node id. The routing table also saves other information such as hop count, destination sequence number, source & destination address. After this, the third phase of algorithm starts as Investigation where the source sequence number of current and earlier request is taken into consideration and then difference between them is computed. In case thesource sequence number of the present route request is too high in comparison with the earlier request then the node from which the current route request received is regarded to beadversarial. This RREQentry is removed from route routing table.

III. COMPARISON ANALYSIS

S. No	Reference	Method	Merits	Demerits
1.	Gupta et.al, (2011).	Black hole Avoidance Protocol (BAAP)	It employs an extra Legitimacy table for preventingadversarial node	Packet loss in the range of15% to 20% of is observed.
2.	Hayajneh et al, (2000).	DeWorm scheme	It has the capability of identifying different kinds of wormhole attacks that includes physical layer wormholes	It does not discard the wormhole after its detection.
3.	Jian-Ming Chang et.al, (2015).	Cooperative Bait Detection Scheme(CBDS)	Higher packet delivery ratio Lesser routing overhead	It is not desirable for different collaborative attacks on MANETs.
4.	Ngai et al. (2006)	Network flow graph based intrusion detection	Greater detection accuracy Lesser routing overhead	Efficient statistical algorithms are needed for detecting data inconsistency and thereby locating themalicious nodes correctly
5.	Kalia andMunjal,	Fuzzy based control scheme	It attains abig true positive rate	Greater communication overhead
6.	Weerasing he and Fu,	Modified AODV protocol	Decent performance in terms of better throughput rate and minimal packet loss percentage	It is capable of detectingjust the collaborative black hole nodes.
7.	Abbas et.al, 2012.	Lightweight sybil attack detection	It identifies the Sybil identities with good accuracy even while moving.	At times,it may identify a normal node to be a Sybil node
8.	Yu et.al (2009).	Secure Routing Protocol	Greater packet delivery ratio It minimizes the link breakage rate during implementation It gives an increased prediction accuracy	It only identifies the Byzantineattacks

9.	Shakshuki et.al, 2013.	EACK Scheme	It attains agreater malicious-behavior-detection rate	hybrid cryptography methodologies are needed in order to further minimize the network overhead owing to digitalsignature
10.	Rathiga et.al, 2016.	hybrid black/gray hole detection approach	It attains ahigherthroughput, packet drop rate, packet delivery ratio and routing overhead.	It does not consider mobility and traffic factorswhile identifying thedangerous node.
11.	Gandhewar et.al, (2012)	AODV based Detection and prevention of sinkhole attack	Higher throughput, PDR Lesser end to end delay and Packet loss	An effective scheme is needed in order to boost the detection rate.

IV. CONCLUSION

Mobile Ad Hoc Networks are capableofestablishing networks on the run in a hostile environment where it might not feasible to implement a conventional network infrastructure. When ad hoc networks are greatly promising, there are still severalissues that areyet to be overcome. Security is a vital feature for the implementation of MANET. In this research work, the challenges and solutions of the routing security attacks are overviewed in mobile ad hoc networks. Those research techniques are explained in addition to their pros and cons in detailto obtain the efficiency of all the algorithms. Severalmethodologies are studied with which few of the collaborative attacks can be fought back with and it is possible to have easierdetection in many of the attacks. But all of the earlier approaches are susceptible to an entire set of collaborative attacks. This will be taken into consideration in future.

REFERENCES

[1] Hong, X., Xu, K., and Gerla, M. (2002), "Scalable routing protocols for mobile ad hoc networks", IEEE network, Vol.16, No.4, pp.11-21.

[2] C.E. Perkins, E.M. Royer, S.R. Das and M.K. Marina, " Performance comparison of two on-demand routing protocols for ad hoc networks", IEEE Personal communications, Vol.8, No.1, 2001, pp.16-28.

[3] M. Mauve, J. Widmer, and H. Hartenstein, "A survey on position-based routing in mobile ad hoc networks", IEEE network, Vol.15, No. 6, 2001, pp.30-39

[4] . P. Papadimitratos and Z.J. Haas, "Secure routing for mobile ad hoc networks", In Conference on the SCS Communication Networks and Distributed Systems Modeling and Simulation (CNDS), San Antonio, TX, 2002, pp.193-204.

[5] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks", IEEE Wireless communications, 2007, Vol. 14, No. 5.

[6] S. Banerjee, "Detection/Removal of Cooperative Black & Gray Hole Attack in MANETs", In proceedings of the World Congress on Engineering & Computer Science 2008.

[7] N. Khemariya and A. Khuntetha, "An efficient algorithm for detection of black hole attack in AODV based manets", International Journal of Computing. Application. 2013, Vol. 66, pp. 18–24.

[8] S. Gupta, S. Kar and S. Dharmaraja, "BAAP: black hole attack avoidance protocol for wireless network", In 2nd International Conference on Computer and Communication Technology (ICCCT), 2011, pp. 468-473.

[9] T. Hayajneh, P. Krishnamurthy and Tipper, D, "Deworm: A simple protocol to detect wormhole attacks in wireless ad hoc networks", In Third International Conference on Network and System Security, 2009, pp. 73-80.

[10] J.M. Chang, P.C. Tsou, I. Woungang, H.C. Chao and C.F. Lai, "Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach", IEEE systems journal, 2015, Vol. 9, No. 1, pp. 65-75.

[11] E.C.H. Ngai, J. Liu and M.R. Lyu, "On the intruder detection for sinkhole attack in Wireless Sensor networks", IEEE communication Society matter expert, Published in IEEE 2006, 3383- 3389.

[12] K. Nishu and M. Kundan, "Multiple Black Hole Node Attack Detection Scheme in MANET by Modifying AODV Protocol", International Journal of Engineering and Technology, Vol. No. 3, 2013.

[13] K.G.H.D. Weerasinghe and Fu, H, "Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation", 2008, Vol. 2, No. 3,

[14] S. Abbas, M. Merabti, D. Llewellyn-Jones and K. Kifayat, "Lightweight sybil attack detection in manets", IEEE systems journal, 2013, Vol. 7, No. 2, pp. 236-248.

[15] M. Yu, M. Zhou and Su, W, "A secure routing protocol against byzantine attacks for MANETs in adversarial environments", IEEE transactions on vehicular technology, 2009, Vol. 58, No. 1, pp. 449-460.

[16] E.M. Shakshuki, N. Kang and T.R. Sheltami, "EAACK—a secure intrusion-detection system for MANETs", IEEE Transactions on industrial electronics, 2013, Vol. 60, No. 3, pp. 1089-1098.

[17] P. Rathiga and S. Sathappan, "Hybrid detection of Black hole and gray hole attacks in MANET", In International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), 2016, pp. 135-140.

[18] Gandhewar, N. and Patel, R, "Detection and Prevention of inkhole attack on AODV Protocol in Mobile Adhoc Network", In Fourth International Conference on Computational Intelligence and Communication Networks (CICN), 2012, pp. 714-718.

Author Profile

"**PVS SIVA PRASAD** is a research scholar in the department of Computer Science and Engineering at Rayalaseema University, Kurnool, and Andhra Pradesh. He received his M.tech (CSE) in 2002 from IETE. His current research interests are Wireless Communications, Swarm intelligence algorithms. He is a Certified Trainer from Heartfulness Institute where research of self through meditation is carried out. "