ISSN 22773061

Review of Acknowledgment Based Techniques for Detection of Black Hole/Gray Hole Attacks in MANETs

Rajveer Kaur
Department of Computer Science & Engineering
Radiant Institute of Engineering & Technology, Abohar, Punjab (India)
er.rajveerdhaliwal@gmail.com

Dr. Shaveta Rani
Department of Computer Science & Engineering
Punjab Technical University Giani Zail Singh Campus, Bathinda, Punjab (India)
garg_shavy@yahoo.com

Dr. Paramjeet Singh
Department of Computer Science & Engineering
Punjab Technical University Giani Zail Singh Campus, Bathinda, Punjab (India)
Param2009@yahoo.com

ABSTRACT

In Mobile Ad hoc NETworks (MANETs) nodes communicate via wireless links, without any fixed infrastructure like base stations, central servers or mobile switching. Each node in MANET can act as a host or as a router. Due inherent characteristics like decentralization, self configuring, self -organizing networks, they can be deployed easily without need of expensive infrastructure and have wide range of military to civilian and commercial applications. But wireless medium, dynamically changing topology, limited battery and lack of centralized control in MANETs, make them vulnerable to various types of attacks. This paper focus on network layer packet dropping attacks – Black Hole & Gray Hole attacks in Dynamic Source Routing (DSR) based MANETs and discuss various pros and cons of acknowledgement based techniques for detection of above said attacks.

General Terms

MANET Security, Network layer Attacks, Acknowledgement based techniques

Keywords

MANETs, DSR, node misbehavior, packet dropping, selfish node, malicious node, Black Hole attack, Gray Hole attack

Academic discipline

Computer networks

Subject classification

Wireless network security

Council for Innovative Research
Peer Review Research Publishing System
Journal: ***INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY***
Vol 5, No 3

editor@cirworld.com
www.cirworld.com, member.cirworld.com

1. INTRODUCTION

Mobile Ad hoc NETwork (MANET) is a collection of devices or nodes that communicate via wireless links, without any fixed infrastructure like base stations, central servers or mobile switching. The nodes can move randomly and do not require pre-determined organization of links to communicate. Mobile nodes which are within the radio range to each other can communicate directly through wireless links, whereas the nodes which are far away depend on other nodes to communicate messages. So each node in MANET can act as a host or as a router. MANETs are decentralized, self configuring, self -organizing networks and can be deployed easily without need of expensive infrastructure. Due to these characteristics, MANETs have number of applications like in military where nodes are scattered on battlefield for surveillance mission, in emergency and disaster struck areas where an infrastructure is unavailable or unfeasible to install and for ubiquitous computing for smart homes. MANETs are also used in mobile conferencing for business meetings and seminars involving a large group of people where access points may be absent or inaccessible. Hence MANETs has wide range of military to civilian and commercial applications.

As MANETs are widely used, their security issues have become one of the primary concerns. Due to wireless medium, dynamically changing topology and lack of centralized control, attacker can easily enter into the network, listen or modify the data being sent and then leave the network. Also all the routing protocols in MANETs assume that every node is honest and cooperate in routing the data through themselves. So if a node claims it can reach another node by a certain path or distance, the claim is trusted; similarly, if a node reports a link break, the link will no longer be used. So due to these fundamental characteristics of MANETs, they are vulnerable to various types of attacks [1].

Attacks in MANETs can be classified on the basis of the source of the attacks i.e. Internal or External, and on the behavior of the attack i.e. Passive or Active attack. An external attack is one caused by nodes that do not belong to the network. Internal attacks are initiated by the authorized nodes in the network, and might come from both compromised and misbehaving nodes. Internal nodes are identified as compromised nodes if the external attackers hijack the authorized internal nodes and then use them to launch attacks against the ad hoc networks. Misbehaving nodes are internal nodes which may refuse to forward the packets or may modify the packets to disrupt network functioning. A passive attack does not disrupt the operation of a routing protocol, but snoop's the data exchanged in the network without altering it. An active attack is an attempt to improperly modify data, gain authentication, or procure authorization by inserting false packets into the data stream or modifying packets in transition through the network. All these types of attacks can be performed on any layer.

Routing protocols proposed for MANETs can be categorized to three types i) Proactive Routing Protocols ii) Reactive Routing Protocols iii) Hybrid Routing Protocols

Proactive protocols also known as Table-driven, find the path to every other individual node in the network whether if there is a packet sending request or not, and attempt to maintain consistent up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and any changes in network topology need to be reflected by propagating updates throughout the network in order to maintain a consistent network view. Examples include Destination Sequenced Distance Vector routing protocol (DSDV)[10] and Optimized Link State Routing Protocol (OLSR)[13].Re

active protocols are also known as demand driven protocols. They do not require constant update of paths and they only create routes when desired by the source node that is they don't find route until demanded. Examples of reactive protocols are Ad hoc On-demand Distance Vector Routing protocol (AODV)[12] and Dynamic Source Routing (DSR)[9]

Hybrid routing protocol is combination of proactive and reactive routing protocol. Zone-based Hierarchical Link State (ZHLS) [11] is typical example of hybrid routing protocol.

In this paper, we have chosen one of the reactive protocols, namely Dynamic Source Routing (DSR) protocol. The reason being, it uses source routing, (that is the packet header contains the path to be followed by the packet), as the source node need to know the identity of every intermediate node in the route to destination. It also avoids the need of constantly updating routing information in the intermediate nodes.

2. DYNAMIC SOURCE ROUTING PROTOCOL

DSR[9] uses source routing rather than hop-by-hop routing, with each packet to be routed carrying in its header the complete, ordered list of nodes through which the packet must pass.

The DSR protocol consists of two mechanisms: Route Discovery and Route Maintenance. Route Discovery is the mechanism by which a node S wishing to send a packet to a destination D obtains a source route to D. To perform a Route Discovery, the source node S broadcasts a ROUTE REQUEST (RREQ) packet that is flooded through the network in a controlled manner. When the intermediate node receives the RREQ, it first adds its address to the RREQ, and then rebroadcasts the modified RREQ. When the destination node receives the RREQ, it constructs a RREP (Route Reply), and copies the accumulated route in the RREQ to the RREP, and sends the RREP to the source on the reverse path. If intermediate node has route available to the destination node, it first adds this route to the RREQ, and then constructs a RREP, and sends the RREP to the source on the reverse path.. At last, when the source receives the RREP, it knows

there is a route to the destination node, and copies the route in the RREP to its memory for later use. Route Maintenance mechanism indicates if a source route is broken or if the network topology has changed, such that it can no longer uses its route to the destination. Then S is notified with a ROUTE ERROR (RERR) packet. The sender S can then attempt to use any other route to D already in its cache or can invoke Route Discovery again to find a new route.

In this paper, we focus on network layer packet dropping attack - Black hole and Gary hole attacks in Dynamic Source Routing (DSR) Protocol based MANETs

3. BLACK HOLE / GRAY HOLE ATTACK IN MANETS

A Black hole (attacker) drops all packets instead of forwarding them. Such a misbehaving node can be selfish or malicious. A selfish node do not participate in the routing functions and drops the packets in order to save its resources like battery life or CPU cycles. But a malicious node may drop the packets, modify the routing information or impersonate other nodes with the intention to disrupt the network and affect its availability.

When a node selectively drop the packets instead of dropping all e.g. packets of particular node, drop the packets after every fixed interval or drops the packets randomly then this is called Gray hole attack [2].

In DSR packet dropping attacks that is Black Hole / Gray Hole attack can occur as following:

- Selfish node may drop all the packets or selective packets to save its resources
- For route discovery, when a node sends RREQ, malicious intermediate node can immediately send RREP claiming a fresh route to destination, to attract the traffic and then drop selective or all packets .
- During route discovery, attacker may impersonate itself as destination and then send RREP to source and later on drop all the data packets forwarded by source.

Number of techniques for detection and prevention of packet dropping attacks are proposed by various authors. These techniques are roughly categorized as i) Credit based ii) Reputation based iii) Secure routing iv) Acknowledgement based. This paper discusses acknowledgement based techniques in which receiver of data packet confirms the reception by sending acknowledgement back to sender.

4. LITERATURE SURVEY

Most of the techniques which we are going to discuss have referred the Watchdog and Pathrater proposed by Marti et al.[14]. These techniques form the basis for many of packet dropping detection techniques that were proposed in the recent years. The first technique is the Watchdog that identifies misbehaving nodes while the second technique is Pathrater that helps routing protocols to avoid these nodes. When a node forwards a packet, the node's Watchdog verifies that the next node in the path also forwards the packet. The Watchdog does this by listening promiscuously to the next node's transmissions. If the next node does not forward the packet, it is a misbehaving node. Every time a node fails to forward the packet, the Watchdog increments the failures counter. If the counter exceeds a certain threshold, it determines that the node is misbehaving; this node is then avoided using the pathrater. The watchdog is based on passive feedback that is overhearing, to confirm whether next has forwarded the packet or not. So it has weaknesses, that it might not detect a misbehaving node in the presence of ambiguous collision, receiver collision, limited transmission power, false misbehavior reporting, collusion and partial dropping.

Various authors proposed the following techniques that use active feedback that is acknowledgement, for confirmation of the reception of data packets by a node and have overcome some or all of the weakness of Watchdog.

K. Balakrishnan et al.[3] proposed TWOACK scheme to detect misbehaving links by acknowledging every data packet transmitted over each three consecutive nodes along the path from the source to the destination. Upon retrieval of a data packet, each node along the route is required to send back an acknowledgement packet to the node that is two hops away from it down the route. Process is shown in fig. 1.

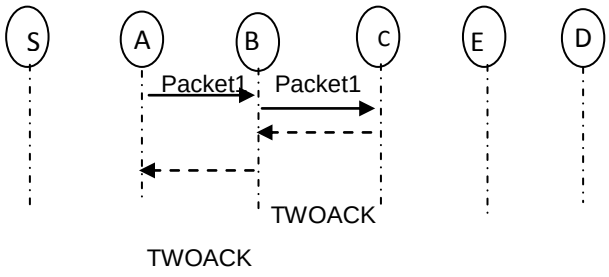

Fig.1: TWOACK Scheme

The retrieval of this TWOACK packet at node A indicates that the transmission of Packet 1 from node A to node C is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, then A send RERR packet to

source to report that link B→C is misbehaving. The same process applies to each three consecutive nodes along rest of the route. The TWOACK scheme has various limitations such as it detects misbehaving link in which either of two nodes may be misbehaving, so well behaved node is also being punish along misbehaved node and also it gives the misbehaving node more chance to drop more packets as it might be connected to different links. TWOACK packets generate extra traffic so increase routing overhead. A malicious node may send false misbehavior report (false RERR packet). In case of false misbehavior report, although node B successfully forwarded Packet1 to node C, node A still reports node B as misbehaving. Malicious node A send this false misbehavior report with intention to declare innocent nodes as malicious. In this technique, a misbehaving node e.g. B may fabricate a TWOACK packet and claim that it was generated by C

K. Balakrishnan et al.[3] proposed S-TWOACK (Selective-TWOACK) scheme, a derivative of the TWOACK scheme, reduces this extra traffic due to TWOACK. In the S-TWOACK scheme, instead of sending back a TWOACK packet every time when a data packet is received, a node waits until a certain number of data packets (through the same triplet) arrive. The node then sends back one TWOACK packet acknowledging multiple data packets that have been received so far.

K. Lui et al [4] proposed the 2ACK scheme which works like TWOACK with differences i) The data packet receiving node sends 2ACK packets as acknowledgment for a fraction of received data packets, while, in the TWOACK scheme, TWOACK packets are sent for every data packet received. Acknowledging a fraction of received data packets gives the 2ACK scheme better performance with respect to routing overhead. 2) The 2ACK scheme has an authentication mechanism to make sure that the 2ACK packets are genuine. The 2ACK scheme suffers from false misbehavior report

Al-Roubaiey et. al. [5] proposed Adaptive ACKnowledgment (AACK) scheme. It is combination of an Enhanced-TWOACK (E-TWOACK), which detects misbehaving node instead of misbehaving link and an end-to end acknowledgment scheme, to reduce the routing overhead of TWOACK. But the AACK mechanism may not work well on long paths that will take a significant time for the end to end acknowledgments. This limitation will give the misbehaving nodes more time for dropping more packets. Also AACK still suffers from the partial dropping attacks (gray hole attacks). It also suffers from false misbehavior report. Further a misbehaving node may send fabricated acknowledgements.

N. Kang et. al. [6] proposed Enhanced Adaptive ACKnowledgement (EAACK) scheme which consists of three parts (i) Acknowledge (ACK) (ii) Secure-ACKnowledgement (S-ACK) (iii) Misbehavior Report Authentication (MRA). ACK is basically an end-to-end acknowledgement scheme. In ACK mode if destination node D successfully receives data packet, it send back an ACK acknowledgement packet along the same route but in a reverse order. Within a predefined time period, if node S receives ACK, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route. S-ACK scheme is an improved version of TWOACK. For each three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgement packet to the first node as done in TWOACK. If the first node in a group does not receive S-ACK then it declare both second and third node as misbehaving nodes and send the report to source node. The source node do not immediately trusts the misbehavior report, EAACK requires the source node to switch to MRA mode and confirm this misbehavior report. With MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report.

N. Kang, et. al.[7] proposed EAACK2, in this acknowledgement packets received in S-ACK phase of EAACK are digitally signed using Digital Signature Algorithm (DSA) to prevent the intermediate node from forging the S-ACK packet. Both the EAACK and EAACK2 cannot detect partial dropping that is Gray hole, during the first phase node may drop packets ase end to end acknowledgement take time

A. Sagar, et. al [8] ,uses improved acknowledgement packets. In this scheme all the nodes in active route are grouped into sets such that set S1 contains first three consecutive node, set S2 contains next three consecutive nodes and so on. First nodes, middle node and last node of a set are referred as LNode, MNode, and RNode respectively and two sets are combined to form groups. Acknowledgement packets are sent in pattern as shown in fig.2

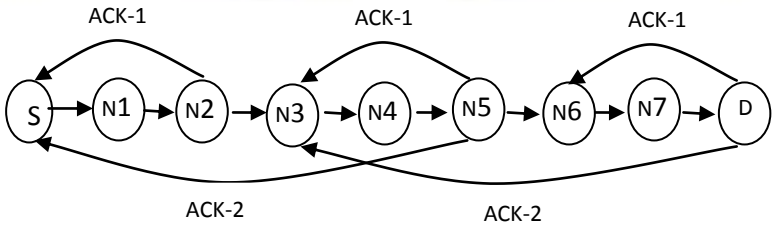

Fig.2: The pattern of sending ACK-1 and ACK-2

If ACK-1 is received within time say T1 then LNode waits for ACK-2 else observes its MNode for time T3 by rating the behavior and if rating falls threshold TS1, LNode declares its MNode as misbehaving nodes and if not, LNode declares its RNode as misbehaving nodes and then flood this information. If ACK-2 is not received within time T2, then after time T2 both MNode of that group automatically goes into promiscuous mode and starts observing their next hop nodes (i.e. RNode) for time T4. As now both MNode are in promiscuous mode and count the number of packets coming into and

going out its RNode and when it is found that number of dropped packets exceeds threshold TS2 within time T4 then that RNode is declared as misbehaving node otherwise LNode of second set is declared as misbehaving node. Finally information of misbehaving node is flooded across the network. This scheme again fails to detect false misbehavior report and forged acknowledgements. This technique can detect both Black hole and Gray hole attacks.

5. COMPARISON

Following is the summarized comparison of above reviewed techniques.

Table 1. Comparison of various techniques

Technique	Routing Overhead	Detect False Misbehavior Report	Prevent Acknowledgement forging	Gray hole detection
TWOACK	Large	No	No	Yes
S-TWOACK	Lesser than above technique	No	No	yes
2ACK	Lesser than TWOACK	No	yes	Yes
AACK	Lesser than above techniques	No	No	N o
EAACK	Same as AACK	Yes	No	No
EAACK2	Same as EAACK	Yes	yes	No
Improved ACK	Least	No	No	Yes

6. CONCLUSION

The schemes AACK [5], EAACK[6], EAACK2[7] and scheme with improved acknowledgement[8] have reduced the routing overhead due to acknowledgement packets as compared to TWOACK[3] and 2ACK[4]. All the above schemes except EAACK and EAACK2 suffer from false misbehavior reports. Except the schemes 2ACK and EAACK2 all the schemes cannot prevent or detect packet dropping by the node which impersonate itself as destination and cannot detect attacks in presence of forged acknowledgements. Future work is to comparatively analyze the simulations of reviewed techniques on basis of various parameters like routing overhead, end to end delay, average attack detection time and detection probability.

REFERENCES

[1]. Sarkar S. K., Basavaraju T.G., Puttamadappa C., 2008, “Ad Hoc Mobile Wireless Networks”. Auerbach Publications.

[2]. Djahel Soufiene, Farid Naıt-abdesselam, and Zonghua Zhang, 2011 “Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges”, IEEE Communications Surveys & Tutorials, Vol 13, No.4, pp 658-672.

[3]. Balakrishnan, K.; Jing Deng; Varshney, V.K., 2005 “TWOACK: preventing selfishness in mobile ad hoc networks”, In Proceedings of Wireless Communications and Networking Conference, 2005 IEEE , vol.4, no., pp. 2137-2142(March 2005)

[4]. Liu K., Deng J., Varshney P.K. and Balakrishnan K., 2007, “An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs”. IEEE Transactions on Mobile Computing, May, 536-550.

[5]. Al-Roubaiey A., Sheltami T., Mahumad A., Shakshuki E., Mouftah H, 2010 AACK: Adaptive Acknowledgement Intrusion Detection for MANET with Detection Enhancement, The 24th International Conference on Advanced Information Networking and Applications (AINA), IEEE Computer Society.

[6]. Kang, N., Shakshuki, E and Sheltami, T., 2010.” Detecting Misbehaving Nodes in MANETs”, In Proceedings of the 12th International Conference on Information Integration and Web-based Applications & Services (iiWAS2010), ACM, pp. 216-222.

[7]. Kang, N., Shakshuki E and Sheltami T. 2011 "Detecting Forged Acknowledgements in MANETs", The 25th International Conference on Advanced Information Networking and Applications (AINA), IEEE Computer Society, Biopolis, Singapore.

[8]. Sagar Aishwarya., Ukey Anand & Chawla Menu, 2010 Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET, International Journal of Computer Science issues, Vol 7, Issue 4, No. 1, pp 12-17.

[9]. Johnson, D.B, Maltz, D.A., and Hu, Y., 2004 The Dynamic Source Routing Protocol for Mobile ad-hoc Networks(DSR), IETF Internet Draft, July 2004.

[10]. Perkins, C. E., and Bhagwat, P. 1994. Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers. In Proc. Of ACM Special Interest Group on Data Comm. (SIGCOMM '94), pp. 234-244.

[11]. Sanzgiri, K., Dahill, B., Levine, B-N., Shields, C. and Belding-Royer, E-M. 1999. A review of current routing protocols for ad-hoc mobile wireless networks. Personal Communications Magazine.

[12].. Perkins, C. E., Royer E. M., Das, S. R., 2002 Ad Hoc On- Demand Distance Vector (AODV) Routing, Internet Draft, draft-ietfmanet-aodv-10.txt.

[13]. Clausen, T. and Jacquet P., 2003 Optimized Link State Routing Protocol (OLSR), *IETF RFC 3626*

[14]. Marti P., Giuli T. J., Lai K., and Baker, M., 2000, "Mitigating Routing Misbehavior in Mobile Ad-hoc Networks", In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom'00), PP. 255-265

Rajveer Kaur has done B.Tech in Computer Science and Engineering from Punjab Technical University, Jalandhar, Punjab, India, in 2002 and M.Tech in Computer Science and Engineering from Punjabi University Patiala, Punjab, India in 2008. She is pursuing Ph.D in Computer Science and Engineering from Punjab Technical University, Jalandhar, Punjab. She has worked in Guru Teg Bahadur Khalsa Institute of Engineering & Technology, Chhapianwali (Malout), Punjab as Lecturer in the dept. of Computer Science and Engineering from August 2002 to July 2008 and as Assistant Professor from August 2008 to July 2011. Presently she is working in Radiant Institue of Engineering & Technology, Abohar ,Punjab since August 2011.She has 1 paper in International refereed journal and 7 papers in National Conferences to her credit. Her research interest includes Computer Networks and Network & Data Security.

Dr. Shaveta Rani received her B. Tech. in Computer Science and Engineering from Punjab Technical University, Jalandhar, Punjab, India, in 1998 and M. S. in Software Systems from Birla Institute of Technology and Science (BITS), Pilani, Rajasthan, India, in 2002. She did Ph.D. in Computer Science and Engineering from Birla Institute of Technology and Science (BITS), Pilani, India, in 2009. Her Ph.D Thesis was "Investigations on Survivability Strategies in WDM Optical Networks". She worked in Giani Zail Singh College of Engineering and Technology, Bathinda, Punjab, India as Lecturer in the dept. of Computer Science and Engineering from Aug. 1998 to May 2005 and as Assistant Professor from May 2005 to May 2008. Presently, since May 2008, she is working as Associate Professor in the Department of Computer Science and Engineering in the same college. She is also looking after the dept. as HoD w.e.f. March 2010. There are 50 research papers to her credit out of which 11 research papers in International refereed Journals, 2 papers in National refereed Journals, 12 publications in International refereed Conference proceedings, rest are in National Conferences. Her research interest includes Computer Networks, Image Processing, Optical Networks and Computing.

Dr. Paramjeet Singh received his B. Tech. in Computer Science and Engineering from Punjab Technical University, Jalandhar, Punjab, India, in 1998 and M. S. in Software Systems from Birla Institute of Technology and Science (BITS), Pilani, Rajasthan, India, in 2002. He did Ph.D. in Computer Science and Engineering from Birla Institute of Technology and Science (BITS), Pilani, India, in 2009. His Ph.D Thesis was "Investigations on Routing and Wavelength Assignment Algorithms in WDM Optical Networks". He worked in Giani Zail Singh College of Engineering and Technology Bathinda, Punjab, India as Lecturer in the dept. of Computer Science and Engineering from September 1998 to May 2005 and as Assistant Professor from May 2005 to May 2008. Presently, since May 2008, he is working as Associate Professor in the Department of Computer Science and Engineering in the same college. He also worked as HoD in the dept. of Computer Science and Engineering of Giani Zail Singh College of Engineering and Technology, Bathinda, Punjab, India from Dec. 2006 to March 2010. There are 51 research papers to his credit out of which 11 research papers in International refereed Journals, 2 papers in National refereed Journals, 12 publications in International refereed Conference proceedings, rest are in National Conferences. His research interest includes Computer Networks, Computer Graphics, and Software Engineering.