ISSN:0975-9646

Dilip Kumar Thumu et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (5) , 2015, 4313-4317

Detecting Malfunctioning Nodes in Mobile Ad hoc Networks by using EAACK

Dilip Kumar Thumu[1], R.Vasavi[2] A. Kousar Nikhath[3]

[1]*M.Tech Student (SE), VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India*

[2]*Assistant Professor (CSE), VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India*

[3]*Assistant Professor (CSE), VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India*

***Abstract*— Mobile Ad hoc NETwork (MANET) is considered as network without infrastructure where communication between the mobile nodes solely depends on the routing protocols which work on assumption that nodes are fully cooperative. In the presence of malfunctioning nodes, most of the routing protocols show dropped performance and in some case whole of the network fails. Malfunctioning nodes interrupt the data flow by either by dropping or refusing to forward the data packets thus forcing routing protocol to restart the route-discovery or to select an alternative route if available which may again include some malfunctioning nodes, thereby forming a loop, enforcing source node to conclude that data cannot be further transferred. In this paper, a new reputation based approach is proposed which deals with such malfunctioning nodes and can be integrated on top of any source routing protocol Proposed approach consists of detection and isolation of misbehaving nodes and based on sending acknowledgement packets back for reception of data packets.**

***Index Terms*—AACK, EAACK, MANET, WATCH DOG.**

I. INTRODUCTION

MANET consists of wireless mobile nodes that form a temporary network without the aid fixed infrastructure or central administration. Nodes can communicates directly to other nodes within their transmission range. Nodes outside the transmission range are communicated via intermediate nodes such that it forms a multihop scenario. In multi-hop transmission, a packet is forwarded from one node to another, until it reaches the destination with the help of using routing protocol. For proper functioning of the network cooperation between nodes is required. Here cooperation refers to performing the network functions collectively by nodes for benefit of other nodes. But because of open infrastructure and mobility of nodes, noncooperation may occurs which can severely degrades the performance of network.

MANET is vulnerable to various types of attacks because of open infrastructure, dynamic network topology, lack of central administration and limited battery-based energy of mobile nodes. These attacks can be classified as external attacks and internal attacks. Several schemes had been proposed previously that solely aimed on detection and prevention of external attacks. But most of these schemes become worthless when the malicious nodes already entered the network or some nodes in the network are compromised by attacker. Such attacks are more dangerous as these are initiated from inside the network and because of this the first defense line of network become ineffective. Since internal attacks are performed by participating malicious nodes which behave well before they are compromised therefore it becomes very difficult to detect.

Routing protocols are generally necessary for maintaining effective communication between distinct nodes. Routing protocol not only discovers network topology but also built the route for forwarding data packets and dynamically maintains routes between any pair of communicating nodes. Routing protocols are designed to adapt frequent changes in the network due to mobility of nodes. Several ad hoc routing protocols have been proposed in literature and can be classified [1] into proactive, reactive and hybrids protocols.

The basic problem with most of the routing protocols is that they trust all nodes of network and based on the assumption that nodes will behave or cooperate properly but there might be a situation where some nodes are not behaving properly. Most adhoc network routing protocols becomes inefficient and shows dropped performance while dealing with large number of misbehaving nodes. Such misbehaving nodes support the flow of route discovery traffic but interrupt the data flow, causing the routing protocol to restart the route-discovery process or to select an alternative route if one is available. The newly selected routes may still include some of misbehaving nodes, and hence the new route will also fail. This process will continue until the source concludes that data cannot be further transferred. Proposed work focus on such misbehavior for its detection and isolation from network.

II. RELATEDWORK

Due to the limitations of most of MANET routing rules, nodes MANET are reluctant on other nodes cooperation to relay data. This dependency facilitates an attacker oppor-tunity to have its impact on network by compromising one or more nodes. To tackle this problem, it arises the need of enhancing the security level of MANETs.

2.1 Watchdog:

Marti, Giuli, and Baker [6] proposed two techniques, Watchdog and Path rater, to be added on top of the standard routing protocol in adhoc networks. Dynamic Source Routing protocol (DSR) is chosen for the discussion to explain the concepts of Watchdog and Path rater. The watchdog method detects misbehaving nodes. The

watchdog identifies the misbehaving nodes by eavesdropping on the transmission of the next hop. A path rater then helps to find the routes that do not contain those misbehaving nodes. In DSR, the routing information is defined at the source node. This routing information is passed together with the message through intermediate nodes until it reaches the destination. Therefore, each intermediate node in the path should know who the next hop node is. Figure: shows how the watchdog works.

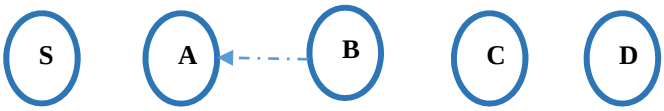

Figure 1. Figure: How watchdog works: Although node B intends to transmit a packet to node C, node A could overhear this transmission.

Assume that node S wants to send a packet to node D, and there exists a path from S to D through nodes A, B, and C. Consider now that A has already received a packet from S destined to D. The packet contains a message and routing information. When A forwards this packet to B, A also keeps a copy of the packet in its buffer. Then, A listens to the transmission of B to make sure that B forwards to C. If the packet overheard from B (represented by a dashed line) matches that stored in the buffer, it means that B really forwards to the next hop (represented as a solid line). It then removes the packet from the buffer. However, if there's no matched packet after a certain time, the watchdog increments the failures counter for node B. If this counter exceeds the threshold, A concludes that B is misbehaving and reports to the source node S. The watchdog is implemented by maintaining a buffer of recently sent packets and comparing each overheard packet with the packet in the buffer to see if there is a match. If so, the packet in the buffer is removed and forgotten by the watchdog, since it has been forwarded on. If a packet has remained in the buffer for longer than a certain timeout, the watchdog increments a failure tally for the node responsible for forwarding on the packet. If the tally exceeds a certain threshold bandwidth, it determines that the node is misbehaving and sends a message to the source notifying it of the misbehaving node. The watchdog technique has advantages and weaknesses. DSR with the watchdog has the advantage that it can detect misbehavior at the forwarding level and not just the link level. Watchdog's weaknesses are that it might not detect a misbehaving node in the presence of

- Ambiguous collisions,
- Receiver collisions,
- Limited transmission power,
- False misbehavior, Collusion, and
- Partial dropping.

The ambiguous collision problem prevents A from overhearing transmissions from B. A packet collision can occur at A while it is listening for B to forward on a packet. A does not know if the collision was caused by B forwarding on a packet as it should or if B never forwarded the packet and the collision was caused by other nodes in A's neighborhood. Because of this uncertainty, A should not immediately accuse B of misbehaving, but should instead continue to watch B over a period of time. If A repeatedly fails to detect B forwarding on packets, then A can assume that B is misbehaving.

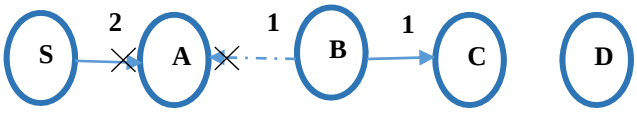

Figure 2. *Ambiguous collision*, Node A does not hear B forward packet 1 to C because B's transmission collides at A with packet 2 from the source S.

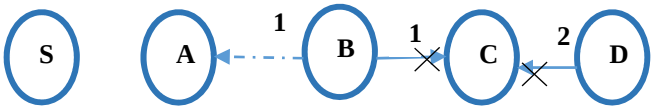

Figure 3. *Receiver collision*, Node A believes that B has forwarded packet 1 on to C, though C never received the packet due to a collision with packet 2.

In the receiver collision problem, node A can only tell whether B sends the packet to C, but it cannot tell if C receives it. If a collision occurs at C when B first forwards the packet, A only sees B forwarding the packet and assumes that C successfully receives it. Thus, B could skip retransmitting the packet. B could also purposefully cause the transmitted packet to collide at C by waiting until C is transmitting and then forwarding on the packet. In the first case, a node could be selfish and not want to waste power with retransmissions. In the latter case, the only reason B would have for taking the actions that it does is because it is malicious. B wastes battery power and CPU time, so it is not selfish. An overloaded node would not engage in this behavior either, since it wastes badly needed CPU time and bandwidth. Thus, this second case should be a rare occurrence

2.2 The TWO ACK Scheme

The TWOACK scheme[8] can be implemented on top of any source routing protocol such as DSR. This follows from the fact that a TWOACK packet derives its route from the source route established for the corresponding data packet. The TWOACK scheme uses a special type of acknowledgment packets called TWOACK packets, which are assigned a fixed route of two hops (or three nodes) in the direction opposite to that of data packets.

Figure 1 illustrates the operational details of the TWOACK scheme. Suppose that the process of Route Discovery has already yielded a source route [S → N1 → N2 → N3 → ⋯ → D] from a source node S to destination node D. For instance, when N1 forwards a data packet to N2, to be forwarded on to N3, N1 has no way of knowing if the packet reached N3 successfully or not. Listening on the medium, as suggested in [6], would only tell N1 whether N2 is sending out the packet or not.1 However, the reception status at N3 is unclear to node N1. The possibility

of collisions at both N1 and N3 makes the overhearing technique vulnerable to medium access problems and false detections [6].

The TWOACK scheme is designed to solve these problems: when N3 receives a data packet, it sends out a TWOACK packet over two hops back to N1, carrying the packet ID of the corresponding received data packet. The route [N3 → N2 → N1] for the TWOACK packet is extracted from the source route of the original data packet. The aim of the TWOACK packet is to notify N1 that the data packet has successfully reached a node that is two-hop away, namely N3. Such a procedure will be carried out by every set of three consecutive nodes, termed triplet, along the source route.

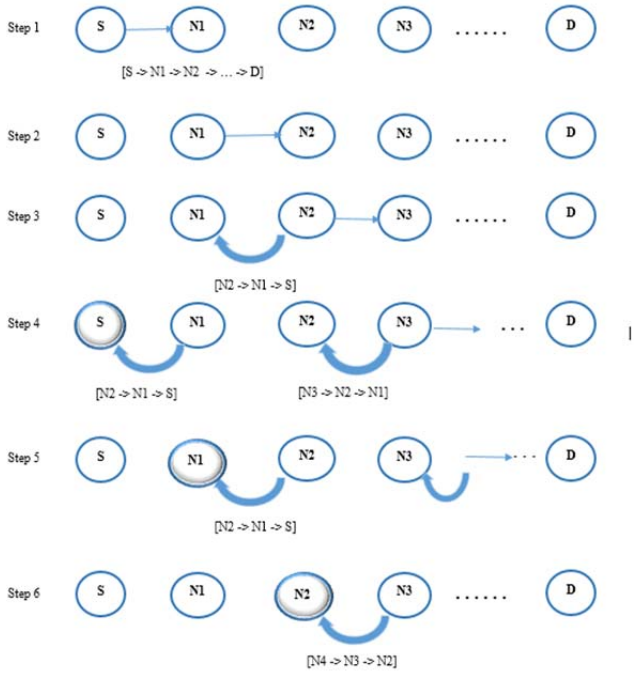

Figure 4: TWOACK Scheme

TWO ACK fails in:

1. Routing Overhead
2. It detects misbehaving links rather than misbehaving nodes
3. False misbehaviour report
4. Forged acknowledgement packet

2.3 AACK :

Based on TWOACK, Sheltami et al. [8] proposed a new scheme, namely AACK which is the combination of TACK (identical to TWOACK) and end to end acknowledgement (ACK). Compared to TWOACK, AACK significantly reduces the network overhead by maintaining the same network throughput. In ACK, the source sends data packet to destination via intermediate nodes. After receiving the packet the destination acknowledges in reverse order. Within predefined time period, if the source receives the ack packet then the packet transmission from source to destination is successful. Otherwise the source will switch to TACK mode by sending TACK and TWOACK still suffer from false misbehavior report problem. i.e., the malicious node may send false report to the source. Hence it is crucial to authenticate the ack packet. To address this problem Enhanced AACK (EAACK) mechanism is introduced, which uses the concept of Digital Signature.

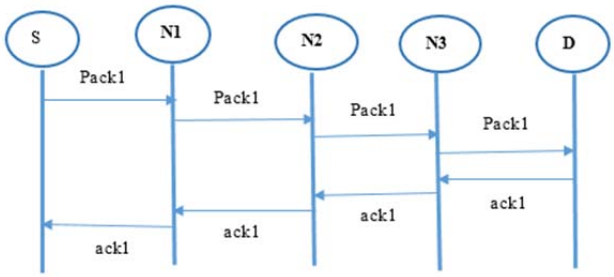

Figure 5:ACK Scheme

III. SCHEME DESCRIPTION

In this section we describe our proposed scheme EAACK in detail [2]. EAACK consists of three parts, namely, ACK, SACK (Secure ACKnowledgement) and MRA (Misbehaviour Report Authentication). In our proposed scheme, we assume that the link between each node is bidirectional and source and destination nodes are authentic.

A. *ACK:*

As discussed above ACK is basically end to end acknowledgement scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce the network overhead when no network misbehavior is detected. As represented in fig 5, in ACK mode, node *S* first sends out an ACK data packet p*ack1* to the destination node *D*. If all the intermediate nodes in the path are cooperate then node *D* successfully receives the packet p*ack1*.Now the destination *D* has to send back an ACK packet *ack1* to the *S* along the same path, within a predefined time. If *S* receives the *ack1* then the packet transmission is successful and there is no intruder existed in the network. Otherwise *S* switches to S-ACK mode by sending ACK data packet.

Packet type	Packet flag
General data	00
ACK	01
S-ACK	10
MRA	11

TABLE I: PACKET TYPE INDICATORS

B. *Secure ACK:*

The S-ACK scheme is improved version of TWOACK scheme proposed by Liu *et al.* [7] .S-ACK scheme detect by acknowledging every data packet transmitted over every three consecutive nodes along the path from source to destination. Every node along the path need to send back a secure ack packet to the current node to the node which is 2hop away from it back.

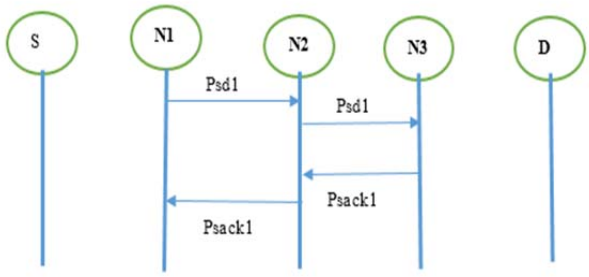

Figure 6: Two Ack Scheme

If node A doesn't receive s-ack packet with in a predefined time period, both B and C are reported as malicious. Then misbehaviour report is generated by A is send to Source. By this source will switch to MRA mode.

C. *MRA (Misbehaviour Report Authentication):*

The MRA scheme is designed to resolve the weakness of Watchdog which was failed to detect the misbehaviours in the presence of false misbehaviour report. The malicious nodes may present the false report as ―candid nodes as nasty or nasty nodes as candid‖. To initiate MRA mode, the source first searches its local knowledge base and seeks for alternative route to the destination node. If the search returns null, source bring into play DSR (dynamic Source Routing) to find another route. Due to the nature of MANETs, it is easy to find several routes for data transmission. After getting the path, the source sends same data packet to the destination via second path. After receiving the ack packet from destination the source node checks whether the ack packet is already existed in its knowledge base or not. If not exists, the report is accepted and valid. Otherwise the report is considered as FMR (False Misbehaviour report) and who generated this report will be treated as Intruder. By adopting MRA mode, EAACK is proficient of detecting misbehaviours despite the existence of FMR.

Here we have two malicious nodes but only one is malicious and other is victim so here two alternate routes is formed which one route consists of one malicious node and another route with another malicious node. Through which route the packet sucesfully reaches reaches it is victim and another is malicious. If already the packet is there in destination the node which claimed the MRA Scheme will be malicious.

D. *Digital Signature*:

In all the three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely on acknowledgment packets to detect misbehaviors in the network. Thus, it is extremely important to ensure that all acknowledgment packets in EAACK are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be vulnerable.

Digital signatures play a vital role in cryptography. It mainly comprises of three Algorithms; [8]

- A *key generation*[9] algorithm that selects randomly a private key uniformly among possible private keys. This algorithm results a set which consists a private key and corresponding public key.
- A *signing algorithm* [9]that results a signature by using private key and message.
- A *signature verifying algorithm*[9] authenticates the message by using public key of the sender and received message.
- The below diagram depicts the procedure followed by the digital signature.

IV. Implementation Of Enhanced Adaptive Acknowledgement And Results

We have used Java programming language to implement the EAACK which consists of three schemes.

i.ACK Implementation:

ACK is basically an end–to–end acknowledgment scheme .The aim is to reduce the network overhead when no network misbehaviour is detected. The figure shows the acknowledgment format.

Received From	Status	Query	TTL
NOD 6483	ACK	dilip	1643

Figure 7:Acknowledgement format

If the acknowledgment is not received with in the time limit then it switches to Secure Acknowledgment Scheme.

ii. Secure Acknowledgment (S-ACK):

In the S-ACK principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect malicious nodes in the presence of receiver collision or limited transmission power. The figure shows the malicious nodes.

Node Name	Message
NOD 5134	Malicious Node
NOD 2160	Malicious Node

Figure 8: Malicious Nodes Table

iii. Misbehavior Report Authentication (MRA):

The main MRA Scheme is to check whether the packet is really not reached to the destination and to find out of two malicious nodes which one is malicious node. so here two alternate routes is formed which one route consists of one malicious node and another route with another malicious node. Through which route the packet successfully reaches it is victim and another is malicious. If already the packet is there in destination the node which claimed the MRA Scheme will be malicious.

V. Conclusion

In this paper we have introduced malicious node detection Technique EAACK. The major threats like false misbehavior report and Partial dropping of packets can be detected by using this scheme. To improve the security of the MANETs we have implemented Digital Signature for Acknowledgement packets so that forge Acknowledgement can be detected which makes MANETs more secure.

REFERENCES

[1] C. Mbarushimana, and A. Shahrabi, "Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad Hoc Networks," in Proc. of the 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW '07), May 2007, pp. 679–684.

[2] EAACK – A Secure Intrusion Detection System for MANETs Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang and Tarek R. Sheltami, Member, IEEE.

[3] D. Johnson, D. Maltz, Y-C. Hu, J. Jetcheva, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", Internet-Draft, February 2002.

[4] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, ―Video transmission enhancement in presence of misbehaving nodes in MANETs,‖ *Int. J. Multimedia Syst.*, vol. 15, no. 5, pp. 273– 282, Oct. 2009.

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

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

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

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

[9] http://en.wikipedia.org/wiki/Digital_signature.

[10] http://www.java2s.com/Tutorial/Java/0490__Security/0320__Digital-Signature-Algorithm.htm

[11] http://www.javatpoint.com/socket-programming

[12] N.Kang, E.Shakshuki, and Sheltami, Detecting misbehaving nodes in MANETS, in Proc. 12thInt. Conf. IIWAS, Nov.2010, pp.216-222.

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

[14] William Stallings, Cryptography and Network Security,Fourth Edition, June 3, 2010.