Journal of Ubiquitous Systems & Pervasive Networks
Volume 7, No. 1 (2016) pp. 13-17

A Guard Node (GN) based Technique against Misbehaving Nodes in MANET

Farid Bin Beshr, Ahmed Bin Ishaq, Saeed Aljabri, Tarek R. Sheltami

KFUPM , Dhahran, Saudi Arabia, 31261

Abstract

In open communication environment such as Ad hoc network, the possibility of having misbehaving nodes is high. The presence of misbehaving nodes could degrade the performance of the overall network. This mandates adopting Intrusion Detection System (IDS) that helps the routing protocol to avoid misbehavior nodes and links. The IDS should feature low overhead controlling packet, high accuracy level and low rate of both false alarms and missed detection rate. There are several IDS techniques proposed in the literature such as Watchdog and End-to-End acknowledgment based system. In this work, we propose a system based on assigning some nodes called "guard nodes" the responsibility of overhearing and reporting the misbehaving nodes. The scheme is proposed to overcome the majority of the drawbacks associated with the Watchdog techniques. We compare and evaluate our proposed scheme against Dynamic Source Routing (DSR) protocol using NS-2 program.

Keywords: *MANET, IDS, DSR, WATCHDOG.TWOACK, EAACK, COLLIDE, MISBEHAVING NODE*

1. Introduction

In Mobile Ad Hoc Network (MANET), a group of mobile nodes collaborate with each other in transmitting their own data packets. One of the main advantages of the MANET network is easy of implementation and configuration as well as the fast deployment. These advantages makes the MANET is a good candidate for emergency, military and medical applications [1] [2]. However, MANET does not have a centralized infrastructure which in turn complicates the network operation like monitoring. Moreover, the low capacity link of MANET brings the need of nodes' cooperation in transmitting the data [3]. There are other characteristic associated with MANET such as quick topology changes, limited nodes' resources (battery power, bandwidth, energy consumptions) and lacking of security functions.

MANET can be classified into two types: open and closed. In the former, the number of users may vary as well as the goals. Users in the open type share the transmission resources to achieve the global connectivity. On the other hand, the nodes in the closed type are governed and controlled by a specific authority in order to reach common goals [3]. One of the main drawbacks of the open MANET type is the potential presence of misbehaving node due to the lack of the physical protection as well as the sharing nature of the transmission resources. A node is marked as misbehaving node when it avails from the network but it refuses to collaborate due to certain reasons. These reasons can be classified into two main types: honest and malicious reasons [4]. The honest reasons are related to collisions, channel errors and buffer overflow, while the black hole, wormhole, and collusion attacks are examples of the malicious attack.

Such misbehaving actions result in low packet delivery ratio and high packet delivery time, which in turn affects the overall performance of the MANET.

Misbehaving nodes have three different activities, which are all defined as misbehaving actions [1]. In the first type, the node participate with network's nodes in routing discovery and maintenance operation, however, it refuse to forward the data packet. In the second type, the node does not contribute in both the routing lookup and data packet transmission.

When the nodes switch its behaviors between the first and second types, the third type of misbehaving actions is present. Usually, there are predefined energy thresholds, which determines the time in which the nodes switch between the first two types of misbehaving activities. It is obvious the importance to detect the first misbehaving type since it is considered as the difficult mode to discover.

There are several examples of misbehaving activities such as intentionality drooping the data packet. Also, the node does not involve in routing creation or block all kinds of packet transmission. In order to detect all types of misbehaving activities, there are several techniques are implemented, which are all called intrusion detection systems (IDS) [5] [6]. In this work, a proposed system based on overhearing guard node is introduced. This scheme overcomes the majority of the drawbacks associated with the Watchdog techniques. The performance measures of the proposed scheme are simulated using NS-2 program

The rest of the paper is outlined as follows: In section 2, we provide background information about the IDS systems. We summarize the related work in the field of Reputation based

* Corresponding author. Tel.: +966 13 874 4146
E-mail: aljabrso@hotmail.com

DOI: 10.5383/JUSPN.07.01.003

and Acknowledgment based IDS scheme in section 3. The proposed IDS scheme is explained in section 4. In section 5, we evaluate the proposed scheme and present the results.

2. IDS

There are several performance factors that need to be considered in designing IDS. For example, the IDS should be efficient in terms of avoiding big overhead controlling packet. In addition, IDS should have a high accuracy level with low rate of both false alarms and missed detection rate. The current IDS techniques are classified into three main categories: Credit Based technique, Reputation Based technique and Acknowledgment based technique [3].

2.1. Credit Based Technique (CBT)

The concept of the CBT is to encourage the node to behave positively by introducing the principle of virtual (electronic) currency. In this scheme, the nodes are paid for giving the services to other nodes in the network. The CBT has three models of operation: Packet Purse Model, Packet Trade Model and SPRITE model. The main difference between the first two models is that, the price of delivering the packet is fixed in the Purse model and it is loaded in the packet frame. In the Trade model, each forwarder buys the packet from the sender by a certain price and sells it to the receiver by higher price that guarantees some profit. In the SPRITE model, a central node called Credit Clearness Service (CCS) usually receives from the network nodes the receipts that are being collected and maintained by the nodes. The CCS determines the charges and credits that need to be given to the service provider nodes. One of the main disadvantages of the CBT is the requirement of extra hardware segment that will maintain the electronic currency.

2.2. Reputation-Based Technique (RBT)

In the RBT, each node is responsible of detecting misbehaving nodes and all nodes cooperate in declaring these selfness actions. This is achieved by broadcasting alarm massaging to the overall network nodes. The main current RBT techniques include Watchdog and CONFIDANT.

3. Related Work

3.1. Watchdog

The node in the Watchdog scheme consists of two units called watchdog and pathrater. The node depends on overhearing (promiscuous mode) in order to detect misbehaving action. In other words, after the node sends the packet to the next hop node, it overhears for some time to determine if its neighbors has transferred the packets to the next node. This is the main function of the watchdog unit. The pathrater part of the node contains a buffer, which has the function of maintaining the ID of the recent transmitted packets. The buffer cleans its databank by deleting the packet's ID, which has been detected during the overhearing operation. The next hope node is declared as a misbehaving if the stored packet's ID stays for a predefined time in the buffer. The misbehaving node is usually avoided in the future by consulting its pathrater cache.

3.2. CONFIDENT

There are four modules in the CONFIDENT technique that work together in order to detect misbehaving actions. These modules are called: monitor, reputation system, path manager and the trust manager. While the main function of the monitor is to perform the overhearing, the reputation system judges the node rating. This can be achieved by receiving the suspicious event reports after any misbehaving event. Based on the frequency of the event reports, the reputation system determines the node rating. The path manager will receive a notification in case of repetitive misbehaving events and it controls the route cache. Accordingly, the trust manager initiates and transmits warning massages in case of declared misbehaving nodes.

3.3. End to-End Acknowledgment

Due to the drawbacks of the Watchdog schemes, several end-to-end acknowledgment techniques have been proposed including the: TWOACK, AACK and EAACK. The disadvantages of the Watchdog are summarized in the below points [7]:

1. Ambiguous collision
2. Receiver collision
3. Limited transmission power
4. False misbehavior report
5. Collusion (cooperation of misbehaving nodes)
6. Partial dropping.

Ambiguous collision: it occurs at the sender node during the overhearing phase when it receives another packet from other node. This results in the collision of the two packets (overhearing packets and the new received packet). As a result, the node cannot determine the successful transmission of the data packet, which is supposed to be delivered by the next hop node.
Receiver Collision: Some time it is possible to declare the successful transmission of the data packet by the next hop node and at the same time, the data does not reach to the destination. This is due to a collision happened at the third hop node. This is called a receiver collision.
Limited transmission power: it is happened when the misbehaving nodes manipulates its transmission power such that it is high enough to be overheard by the previous node. Simultaneously, it is weak to be received correctly by the next node.
False misbehavior report: the misbehaving nodes could generate a fabricated report in which it claims that the next hope did not cooperate in sending the data packet.
Collusion: although sometime the second hop node transmits the packet to the third hop node, it does not report the misbehaving action done by the third hop node. In this case, these two nodes are called colluded nodes.
Partial Dropping: In order to avoid to be announced as misbehaving nodes, the malicious node keeps its score just below the threshold by performing partial dropping.

3.3.1. TWOACK scheme

The TWOACK method works with the Dynamic Source Routing protocol (DSR) since it utilizes the labeled route address in determining the ID receiver of the TWOACK packets [3]. The main idea of the TWACK method is to confirm the reception of the data packet to the third hop nod.

Sending two-hop acknowledgment packet back to the sender can confirm the data reception as shown in figure 1. Here, the third hop nod utilizes the labeled route address for sending the TWOACK packet. In case of not receiving the TWOACK packet after certain timeout and threshold, the complete link (the two and third hop nodes) is considered as a misbehaving link. While the timeout is defined as the maximum time before considering the data packet is dropped, the threshold is the maximum number of lost data packets before considering the link as misbehaving. The misbehaving link is avoided in the future data transmission, which will results in enhancement in the overall network throughput.

The TWOACK scheme solves three drawbacks of the Watchdog method, which are: receiver collision, ambiguous collision and limited transmission power. However, one of the disadvantages of the TWOACK is that it cannot determine the misbehaving node; it determines the misbehaving link instead. Moreover, its extra overhead represented in the TWOACK packet is considered as one of the main system drawback. This is especially related to the fact that each node needs to send two acknowledgment packets in the opposite data direction. One acknowledgment packet is sent to the one hop node and another one is sent to the two-hop node.

The deficiency of the extra overhead can be partially solved by applying the modified TWOACK method, which is called Selective TWOACK (S-TWOACK). In this scheme, the TWOACK packet actually acknowledges multiple data packet instead of single data packet.

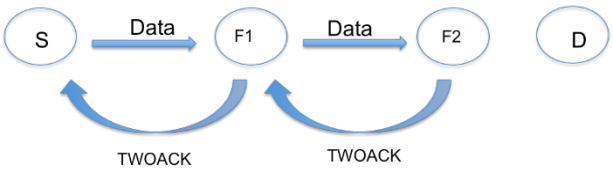

Fig. 1. TWOACK scheme

3.3.2. AACK

There is another method proposed to solve the problem of the extra overhead packet introduced in the TWOACK sachem, which is called AACK [8]. This technique consists of two modules: TACK and ACK. The TACK is identical to the TWOACK method while the ACK is simply an end-to-end acknowledgment technique (i.e. Final Destination sends acknowledgment pack back to the source). The source starts with ACK scheme and if it does not receive a destination acknowledgment after predefined timeout, it switches to the TACK scheme. Although this technique solves the problem of the extra overhead, it still has the deficiency as the TWOACK, which is the disability of detecting false misbehavior report s and forged acknowledgment packet.

3.3.3. EAACK

The main objective of the EAACK is to overcome the previous method's drawback of the AACK in terms of incapability of detecting false misbehavior report [9]. The EAACK consists of three schemes. The first one is the regular end-to-end Acknowledgment (ACK). In case of not receiving the destination acknowledgment within predefined time duration, the system will switch to a modified and secured TWOACK scheme called S-ACK. In S-ACK, each three consecutives nodes collaborate in order to identify the misbehaving nodes instead off misbehaving link. In order to authenticate the received misbehaving report, source shall double check with the destination through alternative route if the packet was received or not. This is the third module of the EAACK scheme called Misbehavior Report Authentication (MRA). Moreover, the EAACK applies the digital signature methodology for each acknowledgment packet. As a result, each acknowledgment packet is authenticated and uncorrupted.

4. The proposed scheme

The proposed scheme is based on the DSR protocol. The principle of the proposed scheme is to delegate the overhearing responsibility to an independent node called a Guard Node (GN) rather than the sender. The idea behind this principle is to overcome the drawbacks of the watchdog technique.

In DSR, a node may cache multiple routes to a destination through the route discovery phase as well as through the overhearing of the routing information destined to others. These multiple routes can be utilized to react to the error routes due to the node mobility, or to avoid the overhead of reinitiating a route discovery to a destination [10].

A GN is the node that can overhear the data transmission from one node or more within the path of the destination. These GNs are selected by the source based on the returned routes during the discovery phase as well as the cached routes. GNs should cover the whole nodes within the path except the source and the distention. The source selects the lowest number of GNs to avoid the overhearing effect on the node such as energy consumption [11]. It is possible that S may be unaware of the any neighbor for a node within the path. Consequently, S asks that node to send its neighbors. One of the neighbors will be selected to be a GN for that uncovered node.

Figure 2 shows how the proposed scheme works. Initially, the source S broadcasts a route request (RQ) in the network asking about the path to the destination D. A route reply (RR) with the path F_1- F_2- F_3- D is returned to S. Then, S looks up its cache to select the lowest number of GNs that can capture the traffic at the forwarder nodes F_1, F_2, and F_3. Based on the cached path, F5 and F6 are selected as GNs of F1 and F2 respectively.

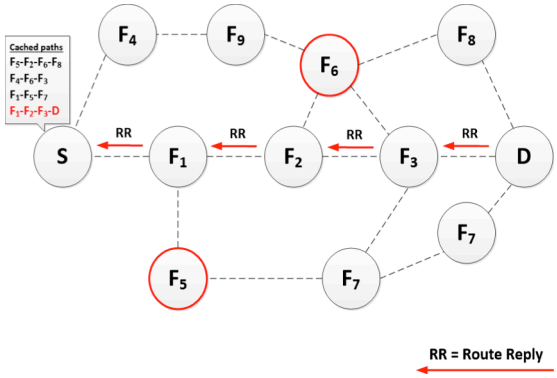

Fig. 2. The proposed approach

At the beginning of the data transition phase, S sends a control packet to the GNs to start overhearing the traffic at the corresponding forwarder nodes. S considers a packet is missed when it does not receive an end-to-end acknowledgment from D during a certain time. S requests each GN to provide the corresponding LF of a missed packet based on the PID. Thus, S can infer who does not forward the packet. Consequently, S broadcasts a message that informs other nodes to remove the malicious node from their paths.

A GN maintains an observation table as seen in table 1, for the captured traffic of the corresponding forwarder nodes. It

includes packet ID PID and last forwarder LF. A GN just needs to keep the last forwarder of the packet even though it captures more than one forwarder.

Table 1: Observation table

PID	LF

5. Performance Evaluation

The proposed scheme has been evaluated using NS2 simulator (NS2) versions 2.34. The same experiments have been conducted to AACK scheme, TACK scheme, and DSR protocol.

5.1. Simulation Setup

We used 50 node scattered within 670X670 meters each moves with maximum speed 1 m/s for low speed scenario and 20 m/s for high speed scenario. We used 10 CBR traffic sources and each runs 4 packets/second as data rate. Packet size is equal to 512 bytes. The misbehaving nodes vary from 0% up to 40% with 10% increments.

Table 2: Simulation Parameters

Parameter	Value
Number of nodes	50
Simulation area	670 meter X 670 meter
Simulation time	900
Mobility model	Random waypoint with pause time 0
Speed range	Low speed (0.1-1), High speed (0.1-20) m/s
Traffic type	CBR
Maximum connections	10
Packet size	512 bytes
Packet rate	4 packets/second
Query Time out	0.5 seconds

The presented results are an average of 10 runs with different seeds. Simulation parameters are shown in Table 2. Parameter Query time out is set initially to 0.5 seconds. This parameter is specifying the delay after which a query packet will be sent to guard nodes to ask them about a specific packet.

5.2. Results and Discussion

We used two metrics to evaluate the protocol performance, packet delivery ratio (PDR) and routing overhead (ROH) and computing as in the following:

$$PDR = \frac{\sum Received\ packets\ at\ destinations}{\sum Sent\ packets\ by\ sources}$$

$$RoH = \frac{\sum Routing\ transmissions}{\sum Data\ \ transmissions + \sum Routing\ transmissions}$$

We run two different sets of experiments using low and high mobility. We evaluated the proposed scheme against original DSR protocol to see the effect of the new scheme in protocol behavior.

Figure 3 shows the packet delivery ratio of both DSR and our scheme, GUARD. When no misbehaving nodes exit, both GUARD and DSR performs similarly with high packet delivery ratio. However, as the number of misbehaving nodes increase the delivery ratio of DSR decrease. Also, GUARD delivery ratio decrease, however, it is ability to detect misbehaving nodes improves its packet delivery ratio.

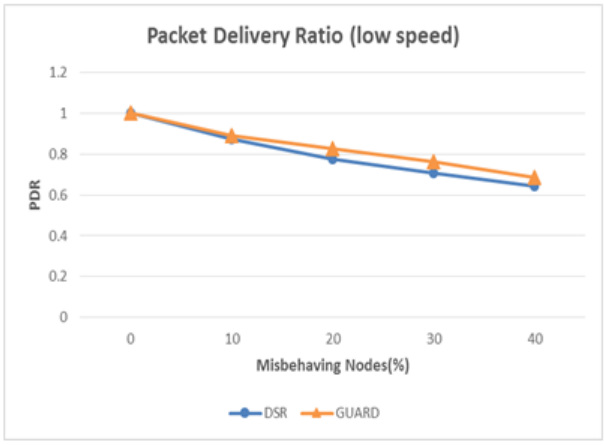

Fig. 3. Packet delivery ratio with low speed.

GUARD performance depends mainly on the existence of neighbor node or guards to monitor packets transitions along routing paths.

Figure 4 shows the routing overhead of both DSR and GUARD. As it was expected, DSR produces the least overhead since do nothing to detect or avoid misbehaving nodes. However, in the case of GUARD scheme, higher overhead is noticed since the source communicates with its neighbors to know the misbehaving nodes.

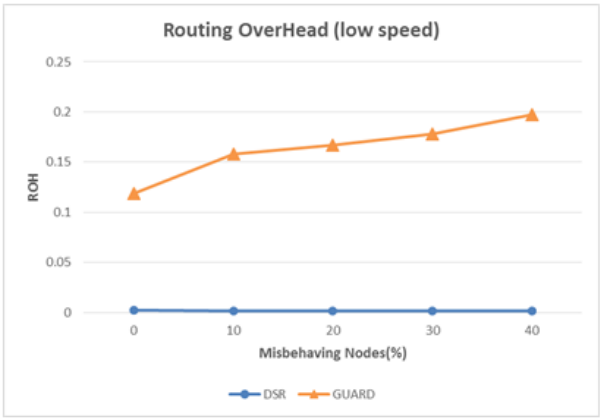

Fig. 4. Routing overhead with low speed.

In GUARD, source node sends queries to ask about missed packets and in response the guard nodes send query replies, which increase the overhead in the network. This feature of GUARD needs more improvement to reduce the overhead, for instance source nodes can piggyback queries within data or DSR control packets to save network bandwidth. It is also applicable in the case of query reply.

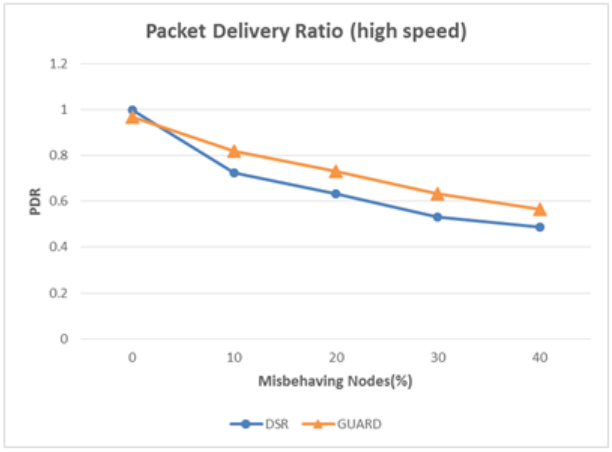

Fig. 5. Packet delivery ratio with high speed.

Figure 5 shows the packet delivery ration of both DSR and GUARD in the high speed scenario. GUARD behaves similar to DSR when no misbehaving nodes exist with little degradation due to overhead and high dynamic network. However, it outperforms DSR and improve the packet delivery ratio as more misbehaving nodes deployed. Compared with low speed scenario, GUARD performs well even when the nodes speed is high.

Fig. 6. Routing overhead with high speed.

Figure 6, shows the routing overhead for both GUARD and DSR. As we discussed before due the nature of GUARD scheme it produces more overhead than in DSR. However, it still acceptable since the network is highly dynamic.

6. Conclusion

In this paper, a GUARD-Node based technique is proposed to defeat the problem of misbehaving nodes in MANET .The proposed scheme is mainly based on the DSR protocol. The principle of the proposed scheme is to delegate the overhearing responsibility to independent nodes called Guard Nodes rather than the sender only. The results showed that GUARD is performing better than DSR even when nodes in high speed. However, the PDR for both GUARD and DSR is affected by almost the same rate as the percentage of the malicious nodes increases. In addition, GUARD is suffering from high overhead, which was expected as penalty of security requirements. For future work, we plan to compare our proposed scheme with other early reviewed works such as Watchdog and TWOACK.

References

[1] Kejun Liu, Jing Deng, Pramod K. Varshney, Kashyap Balakrishnan,. An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 6, NO. 5, MAY 2007

[2] Y. Xiao, X. Shen, and D.-Z. Du (Eds.), "A Survey on Intrusion Detection in Mobile Ad-hoc Networks," Wireless/Mobile Network Security, pp. 170-196, 2006

[3] Balakrishnan K., Jing Deng, Varshney PK. TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks Wireless Communications and Networking Conference, 2005 IEEE (Volume:4)

[4] Deepika Dhiman Neha Sood. Enhanced 2ACK scheme for Reducing Routing Overhead in MANETs International Conference on Parallel, Distributed and Grid Computing 2014

[5] Nan Kang, Elhadi M. Shakshuki, Tarek R. Sheltami,"Detecting Misbehaving Nodes in MANETs" WAS2010, 8-10 November, 2010, Paris, France.

[6] Deepika Goyal1 , Mr. Deepak Kumar Xaxa"An Comparative study and evaluation on performance of Intrusion Detection Schemes in MANET", International Journal of Computer Techniques -– Volume 2 Issue 1, 2015

[7] [Marti, S., 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 (Boston, Massachusetts, United States, August 06 - 11, 2000). MobiCom '00. ACM, New York, NY, 255-265. DOI= http://doi.acm.org/10.1145/345910.345955

[8] A Al-Roubaiey, T. Sheltami, A. Mahmoud, E. Shakshuki, H. Mouftah," AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection Enhancement" 2010 24th IEEE International Conference on Advanced Information Networking and Applications. http://dx.doi.org/10.1109/aina.2010.136

[9] Shakshuki EM, Nan Kang, Sheltami TR. EAACK—A Secure Intrusion-Detection System for MANETs, EEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013

[10] Broch, Josh, David B. Johnson, and David A. Maltz. "The dynamic source routing protocol for mobile ad hoc networks." (1998).

[11] Basu, Prithwish, and Jason Redi. "Effect of overhearing transmissions on energy efficiency in dense sensor networks." Proceedings of the 3rd international symposium on Information processing in sensor networks. ACM, 2004. http://dx.doi.org/10.1145/984622.984652