Novel Evaluation of ACK based IDS Techniques for Dropping Attack in MANETs using OMNET++ Simulator

M. A. Mohamed
Assoc. Prof-Faculty of Eng.
Mansoura, 35511
Egypt

H. S. Mostafa
Assist. Prof. Faculty of Eng.
Mansoura, 35511
Egypt

M. E. Eissa
M.Sc. Student Faculty of Eng.
Mansoura, 35511
Egypt

ABSTRACT
Wireless networking is becoming one of the most important technologies nowadays, allowing users to get services and access information regardless of their location and allows users to communicate with each other wirelessly without depending on any fixed infrastructure. However, MANET works under an assumption that all nodes in the network are collaborating to forward packets which in fact isn't true as there are selfish nodes which refuse to forward the packets to reserve its energy and other resources, also there are misbehaving nodes (attack nodes) which drop packet to harm the network. So, with the presence of the selfish nodes and dropping attack nodes the sureness of the data packet delivery to the destination is absent, therefore, the importance of an intrusion detection system arises to prevent those kinds of nodes from harming the network and make sure that data packet arrives at the destination node. As the importance of the MANET increases, it became a point of interest to the researchers to secure it, so many schemes like Watchdog and Pathrater; Ex-Watchdog; TWOACK; AACK and A3ACK were introduced to achieve this goal. The reference to all techniques is the watchdog technique but it has six weaknesses which are it fails to detect malicious misbehaviors with the presence of the following: (i) partial dropping; (ii) collusion; (iii) false misbehavior report; (iv) limited transmission power; (v) receiver collisions, and (vi) ambiguous collisions. The ACK based techniques were proven to detect malicious misbehaviors with the presence of collaborative attacks, receiver collisions, and limited transmission power .This paper introduces a study of the ability of the ACK based techniques to overcome a major disability in watchdog technique (using omnet++ simulator) which is used to detect malicious misbehaviors with the presence of partial dropping 50%. The importance of choosing partial dropping comes from simulating a real attack scenario, also it is more difficult for the intrusion detection system to detect attackers with partial dropping so, in some way using a partial dropping attack is an evaluation of the strength of the intrusion detection system technique. From this research, it is proven that the ACK based techniques can actually overcome this disability but only with low speed as with low speed the performance is acceptable but with high speed and the presence of collaborative attacks the ACK based techniques have low performance.

General Terms
Ad-hoc Networks, Security

Keywords
Mobile Ad hoc Network (MANETS), Ack-based Intrusion Detection System, Dropping attack, Partial dropping, OMNET++

1. INTRODUCTION
Since the day that the wireless network was invented it became preferred over the wired networks due to its mobility; scalability, and its low cost. By definition, MANET is a collection of mobile nodes equipped with both wireless transmitter and receiver that communicate with each other via bidirectional wireless links either directly or indirectly. Industrial remote access and control via wireless networks are becoming more and more popular these days [1]. One of the most important features in wireless networks is that it allows two nodes to communicate with each other while moving with no problem. This feature comes with a condition which is the nodes must be in each other transmission range, so the moment they become outside each other transmission range the communication is terminated. MANET comes as a solution for this problem by allowing the source nodes to relay on the intermediate nodes to transmit data to the destination node if the destination node is out of source transmission range. So in MANETs the nodes can work as routers where they route the packets of the other nodes.

Ad-hoc networks are decentralized; self-configuring; self-organizing networks which are capable of maintaining communication without depending on any fixed infrastructure, also they can be a standalone networks with no access to the Internet or with an access to the Internet. Because of their features and facilities MANETs have many applications including in military battlefield: Ad-Hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information head quarter [2]. Another new application of MANET is ubiquitous computing for smart homes [3]. Also, MANETs are the solution of choice in the emergency situations where existing infrastructure networks are destroyed or malfunctioned.

As the importance and the applications of the MANET increases its security issue becomes one of important topic for the researchers, e.g. almost all the existing routing protocols in MANETs assume that all nodes in the network are working cooperatively with each other and not maliciously, as a result for this assumption attackers can easily insert malicious or non-cooperative nodes into the network. Also some time nodes in MANETs can choose not to work cooperatively with other nodes just so it can save its battery, so it droppers the data without forwarding it. As a result it became crucial to develop an IDS specially designed for MANETs. The first technique was introduced as an IDS was the Watchdog and Pathrater but it has six weaknesses which is it fails to detect malicious misbehaviors with the presence of the following: (i) partial dropping; (ii) collusion; (iii) false misbehavior report; (iv) limited transmission power; (v) receiver collisions, and (vi) ambiguous collisions. Any other technique came after the

Watchdog tried to solve the six weaknesses. The ACK based techniques was proven to detect malicious misbehaviors with the presence of collaborative attacks, receiver collisions and limited transmission power .This paper introduce a study of the ability of the ACK based techniques to overcome a major disability in watchdog technique which is used to detect malicious misbehaviors with the presence of partial dropping 50%.

In this paper: (i) OMNET++ simulator is used to evaluate the dynamic source routing (DSR) protocol, the TWOACK, the AACK and A3ACK not the NS2 like almost all the papers; (ii) A study of their ability of overcoming the disability in watchdog technique in detecting malicious misbehaviors with the presence of receiver collisions, partial dropping 50%, limited transmission power, and collusion attacks; in all papers a total dropping 100% is used; (iii) the study shows that with high speed, the presence of collaborative attacks and partial dropping the ACK based techniques have low performance, with low speed the performance is acceptable, and (iv) updating the internal code the netattacks_v1.0.0 simulation module in OMNET++ because it work only for INET 2.1.0 which is an old version and doesn't work with the new version of OMNET++, also w have changed the code so the attack node not only drops packets but first processing it and send false acknowledgement to other nodes so it can persuade other nodes that it is working correctly.

The rest of this paper is organized as follow: (i) Section-2: is a brief discussion on the related work; (ii) Section-3: is the problem definition; (iii) Section-4: describes the evaluated techniques; (iv) Section-5: illustrates the performance evaluation including the simulator used, simulation methodology and performance metrics; (v) Section-6: provides the results are discussions; (vi) Section-7: introduces the conclusions and future works and (vii) Section-8: the references.

2. RELATED WORK

2.1 Watchdog and Pathrater

The watchdog and Pathrater technique was introduced by Marti et al.[4], it was added on top of the standard routing protocol to increase the throughput of the network when malicious nodes appear in the network. This method is divided into two parts: watchdog part and Pathrater part. The watchdog part works as an IDS for MANETs to prevent malicious nodes that're done by promiscuously listening to its next hop's transmission. If the node doesn't transmit the packet within a predefined time the watchdog increases its failure counter. At whatever point a node's failure counter surpasses a predefined limit, the Watchdog hub reports it as getting out of hand. When a node reported as a misbehaving node the pathrater which is the other part of the technique work with the routing protocol to avoid the misbehaving nodes in the future transmission. This technique proved itself to be efficient and also to be node detection technique rather than link technique. These advantages made the watchdog technique to be an inspiration to other technique by being based on it or an improvement to it. However, as pointed out by Marti et al. [4], this procedure neglects to recognize malicious misbehaviors activities with the nearness of the accompanying: (i) partial dropping; (ii) collusion; (iii) false misbehavior report; (iv)limited transmission power; (v) receiver collisions, and (vi) ambiguous collisions.

2.2 Ex-Watchdog

Nasser and Chen [5] proposed a technique which is basically an improvement of watch dog and pathrater scheme. This technique aims to solve one of the six weaknesses in the watchdog scheme which is the false misbehavior report. In this scheme, each node maintains a table having members of source address, destination address, and the statistics of the packets forwarded, received and stored. If any node suspected to be misbehaving, then instead of doing with this suspicion, a new route is found to destination excluding suspected node and number of packets received is checked at the destination node. If this number is equal to the number of packets sent, then it is a false misbehavior report and whosoever generated is considered to be malicious .After that, pathrater or works with the routing protocol and update the rating of the node in their corresponding tables. This technique fails to detect the misbehaving node if it is on all the routes from source to destination.

2.3 Dynamic Source Routing (DSR) Protocol

DSR routing protocol can be categorized as an on-demand routing protocol. It is being divided into two parts: route discovery and route maintenance. In the rout discovery part, each node contains a route information cache which can be a path cache or link cache [6]. Whenever a node wants to send a message to another it checks its routing cache if the path forms the source to the destination is present it use it to reach the destination if not it starts a route discovery to find it. The other part of the DSR routing protocol is the route maintenance which provides an assurance that the data is received by the destination, this is done by making every node responsible for confirming that data has been delivered to the next hop node which can be provided by making the next hop node send back an acknowledgement to the source or the forwarder (previous node) as soon as it receives the packet,

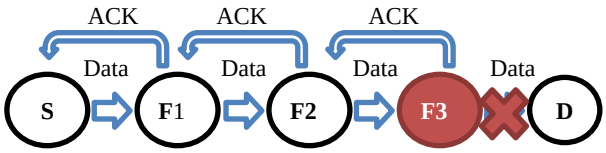

Fig 1: Acknowledgment in DSR protocol

see Figure 1 As can be see if node F3 is a malicious node didn't forward the packet to node D there is no way that node F2 would know that [6, 7].

3. PROBLEM DEFINITION

In this paper, we examine the ability of ACK based techniques to tackle four of the six weaknesses of Watchdog scheme, which are Receiver collisions, partial dropping, limited transmission power, and collusion attack [8].

3.1 Receiver Collisions

Node F1 assure that node F2 has forwarded packet 1 to node F3 by overhearing, but fails to detect that node F3 didn't receive packet A due to a collision of packet A with packet B forwarded by node F4. That means both nodes F2 and F4 are trying to send packet A and packet B, respectively, to node F3 at the same time as shown in Figure 2.

3.2 Limited Transmission Power

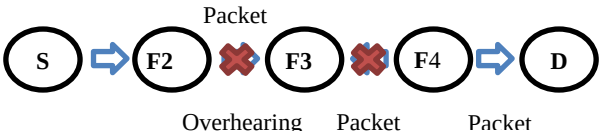

Fig 2: Receiver collisions

To spare energy, a selfish node could confine its transmission power such that the sign is sufficiently solid to be caught by

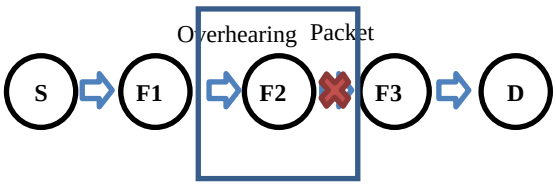

Fig 3: limited transmission power

the past node however too frail to ever be gotten by the true recipient. For instance, node F2 could confine its transmission power so it is sufficiently solid to be caught by node F1 yet too feeble to ever be gotten by node F3, as appeared in Figure 3.

3.3 Collaborative Attacks (Collusion Attacks)

In MANETs multiple misbehaving nodes could cooperate with each other to drop packets instead of forwarding them. For example, nodes F2 and F3 in Fig.4 could cooperative to drop packet A, where node F2 forwards packet A to node F3 but does not report to node F1 when node F3 drops packet A. see Figure 4.

3.4 Partial Dropping

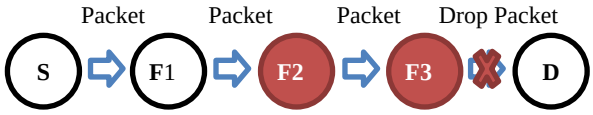

Fig 4: Collaborative attacks

In this case, the attack node chose to drop a percentage of packets to all of it just to confuse the network and to make it difficult for the intrusion detection system to discover its misbehaving behavior. In this study percentage of 50% is chosen. As mentioned the watchdog technique failed to detect dropping attack in the presence of partial dropping. In this study, the ACK based technique is tested whether it can overcome partial dropping or not.

4. THE EVALUATED TECHNIQUES

In this section, we study TWOACK, AACK, A3ACK schemes which work as IDS and compare their functionality with the DSR which doesn't include IDS.

4.1 Two Acknowledgment Scheme (TWOACK)

Balakrishnan et al. [9] propose the TWOACK scheme as a solution to the effect of malicious nodes in MANETs and as an alternative to the watchdog technique to solve the limited transmission power problem and the receiver collision problem. This scheme is created to be on top of the DSR routing protocol. Suppose that node S (source) want to send a message to node D (destination) and it found that the source

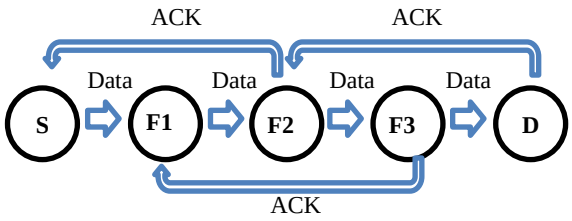

Fig 5: TWOACK mode: Each node is required to send back an acknowledgment packet to the node that is two hops away from it.

route from S to D is S → F1 →F2 → F3 → D where F1, F2, F3 are a forwarders nodes. In this scheme the maintenance part of the DSR routing protocol is altered so instead of making say F2 send an acknowledgment to F1; F3(two hops away form F1) is the one that sends the acknowledgment to F1, in this way F1 makes sure that F2 forwarded the message to F3. If no acknowledgment received at F1 within a predefined timeout F1 suspects F2 to be misbehaving, see Figure 5.

To detect misbehavior, the sender or forwarder maintains a list of data packet IDs that have yet to receive a 2ACK acknowledgment packet from a node two hops away(in our case F3). Each node (F1) contains a separate and a unique list for each forwarding link (F2→ F3) that it is using. Each forwarding link on the list has the following knowledge, see Table 1.

Where F2 and F3are the IP address of the next hop and the next-next hop in the source route; Cmis: counter for the number of times the node suspects a misbehaving; and LIST: list of data packet IDs that still awaiting for 2ACK acknowledgment packets. Every time node F1 doesn't receive an acknowledgment from F3 after a predefined timeout it increases its Cmis counter. When Cmis counter exceeds a certain predefined threshold, F1declares the corresponding link, F2 → F 3, misbehaving delete the link from its route cache, placing the link in the Black and sends to the source an RERR packet to inform it about the same.

Table 1. Data Structure maintained for misbehavior detection

F1	F2	Cmis	List
Next hop node	Next-Next hop node	Misbehavior counter	List of Data Packet IDs Awaiting TWOACsK

4.2 Adaptive Acknowledgment Scheme (AACK)

Sheltami, Al-Roubaie, et al [10] propose the AACK technique as an enhancement scheme of the TWOACK. It is a network layer IDS which is a combination of TWOACK scheme and end to end acknowledgement. It is proposed to solve two of the problems in the watchdog scheme (like TWOACK) but with less routing overhead. Also, it is designed to be a node detection misbehavior scheme instead of the link one (like TWOACK) which will help to detect the exact misbehaving or malicious node and furthermore enhance the performance of the IDS. AACK scheme produce a switching technique so it uses one bit of the reserved field of DSR header to classify the data packets to two types AA and TA data packets where

the source node is the only node that is capable of the switching.

By default the data type is AA which make the acknowledgment model is End-to-End acknowledgment. In this model if a source node S send a message to a destination node D through an active path only the destination node is obligated to send an acknowledgment packet to the source node in the opposite direction of the active route path, see

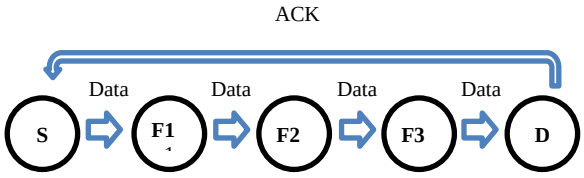

Fig 6: End-to-End ACK

Figure 6. If the source node didn't receive an acknowledgment it suspects that there is a misbehaving or malicious node in the source route, after a predefined number of the missing acknowledgment the source switch the data type is TA which make the acknowledgment model is the enhance TWOACK which is used to find the malicious node.

To enhance the TWOACK technique the misbehaving detection become a node detection instead of link detection to do that any node in the network is classified into three types : source, intermediate and destination, by using this classification any three consecutive nodes in the network can have four possibilities and by knowing the fact that the malicious node exists at the intermediate nodes and the destination node cannot be the misbehaving one the exact malicious node can be found, see Table 2.

Table 2. The selection of malicious node from of any three consecutive nodes

possibilities of any three consecutive nodes	Malicious node
Source→ forwarder 1 → destination	forwarder 1
forwarder 1 → forwarder 2 → destination	forwarder 2
Source → forwarder 1 → forwarder 2	If source receives no acknowledgment forwarder 1 else forwarder 2
forwarder 1 → forwarder 2 → forwarder 3	forwarder 3

4.3 Adaptive Three Acknowledgement Scheme (A3ACK)

Basabaa [11] proposed a scheme that is an extension of the AACK scheme, its main advantage is the detection misbehaving nodes even in the presence of collaborative attacks. A3ACK scheme use a switching technique so it uses two bit of the reserved field of DSR header to classify the data packets to three types AA, TA and THA data packets where the source node is the only node that is capable of the switching.

By default the data type is AA which make the acknowledgment model is End-to-End acknowledgment. In this model if a source node S send a message to a destination node D through an active path only the destination node is obligated to send an acknowledgment packet to the source node in the opposite direction of the active route path. If the source node didn't receive an acknowledgment it suspects that there is a misbehaving or malicious node in the source route, after a predefined number of the missing acknowledgment the source switch the data type is TA which make the acknowledgment model is the enhance TWOACK. If the source node S doesn't receive an acknowledgement packet within a predefined timeout, it has to switch the data type to THA which make the acknowledgment model is A3ACK to detect if there is any two consecutive misbehaving nodes the route path. This is done by making the node send acknowledgment three hops away in the opposite direction see Figure 7.

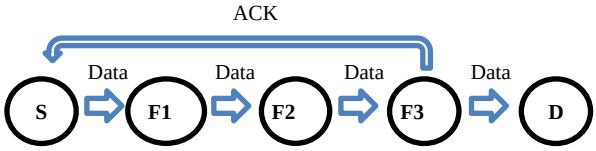

Fig 7:A3ACK mode: Each node is required to send back an acknowledgment packet to the node that is three hops away from it.

5. PERFORMANCE EVALUATION

A description of the simulator, simulation methodology, simulation configurations and performance metrics is discussed in this section.

5.1 Simulator

OMNET++ simulator version 4.6 running on Ubuntu Linux version 15.05 will be used. The system is running on a laptop with processor Core i5 and 4GB RAM.. We also use the INET simulation module version 2.6 which can be considered the standard protocol model library of OMNET++. INET contains models for the Internet stack, wired and wireless link layer protocols, mobility support, MANET protocols, several application models, and many other protocols and components [12]. For the dropping attack we use the netattacks_v1.0.0 simulation module but we update the internal code because it works only for INET 2.1.0 which is an old version and doesn't work with the new version of omnet++, also we change the code so the attack node not only drops packets but first processing it and send false acknowledgement to other nodes so it can persuade other nodes that it is working correctly (collaborative attack).

5.2 Simulation Methodology

To get acceptable information about the performance of all presented schemes, different types of attacks will be used. Two scenarios were proposed to simulate different types of misbehavior or attacks [11]: (i) Scenario-1: In this scenario, we simulated a basic packet dropping attack. Malicious nodes simply drop half of the data packets that they receive. The purpose of this scenario is to test the performance of IDSs

against three weaknesses of Watchdog, which are limited transmission power, and receiver collision in the presence of partial dropping without the presence of collaborative **attacks**. This scenario was evaluated once when the nodes move with low speed and with high speed and (ii) Scenario-2: In this case, malicious nodes drop half of the packets that they receive dropping with the presence of collaborative attacks. The purpose of this scenario is to test the performance of IDSs against four weaknesses of Watchdog, which are limited transmission power, and receiver collision in the presence of partial dropping and the presence of collaborative attacks. This scenario was evaluated once when the nodes move with low speed and with high speed.

5.3 Simulation Configurations

The specifications of the proposed network are [13]: (i) Number of nodes: 50 nodes; (ii) Coverage area: 670 × 670 m; (iii) Mobility type: Random WP Mobility; (iv) Packet length: 512 bytes; (v) Send interval: 0.025s; (vi) Transport layer: UDP protocol; (vii) Application layer for source nodes: UDP Basic Burst; (viii) Application layer for destination nodes: UDP Sink, and (ix) MANET routing protocol: dynamic source routing DSR. Any node in the network consist of an application layer, network layer, NIC layer (which is the MAC layer and physical layer), also it includes the mobility, notification board, routing table and interface table module.

The parameters of the DSR module are shown in Table 3, the parameters of the MAC and psychical layer is in Table.3. Each data point was obtained by running the simulation 10 times with various seed numbers and taking the average value. The misbehaving nodes populace changes from 0% to 40% with 10% additions.

5.4 Performance Metrics

In this study, two performance metrics are used to evaluate the DSR, 2ACK, AACK, A3ACK scheme. The definitions of those metrics are [8]:

5.4.1 Packet Delivery Ratio

This metric demonstrates the capacity of the system to effectively deliver packets to the destination which can be calculated by the proportion of the quantity of the successfully received packets at the destination to the quantity of packets sent by the source.

5.4.2 Routing Overhead

This metrics shows how much the intrusion detection system technique overheads the network with packets so it can actually work which can be calculated by the ratio of routing-related packets in bytes (RREQ, RREP, RERR, AACK, TWOACK, A3ACK,alarms, and Switch) to the total routing and data transmissions in bytes(sent or forwarded packets). That means the acknowledgments, alarms and switching over head is included.

Table 3. Parameters of the DSR module

DSR module parameter	value
Use Network Layer Ack	true
Max Request Rexmt	5
Rexmt Buffer Size	100
Max Maint Rexmt	5
Try Passive Acks	false
Max Salvage Count	3
RREQ Max Visit	5
Promisc Operation	true
Send Buffer Timeout	30s

6. RESULTS AND DISCUSSIONS

In this section the result of both scenario 1 and Scenario 2 in low speed and high speed is shown, also a comparison of this result and the results in [9, 10, 11] (when a total dropping of 100% is used) is discussed to see how much the intrusion detection system is affected when a partial drooping.

6.1 Results of Scenario-1 with Low-Speed Mobility

Total Dropping: (i) PDR of DSR, TWOACK, AACK, A3ACK schemes is close to "1" in case of no malicious nodes; (ii) AACK, A3ACK, and TWOACK outperform both DSR and Watchdog by around 25% in the PDR; (iii) For PDR metric in the presence of small number of malicious nodes, the AACK slightly outperforms the TWOACK scheme, but in the presence of large number of misbehaving nodes (30% and 40%) AACK outperform the TWOACK schemes by approximately 6%; (iv) The PDR of AACK and A3ACKs schemes is almost the same, and (v) The RoH in case of A3ACK scheme is almost the same as in case of AACK scheme which in average is less than the RoH for the TWOACK scheme.

Partial Dropping (50%); As shown in Figure 8 and Figure 9: (i) Packet delivery ratio of DSR, TWOACK, AACK, A3ACK schemes is close to 1 in case of no malicious nodes; (ii) AACK, A3ACK, and TWOACK outperform both DSR by around 30% max in the packet delivery ratio; (iii) For packet delivery ratio metric in the presence of small number of malicious nodes, the A3ACK is the same as the AACK scheme, but in the presence of large number of misbehaving nodes (30% and 40%) A3ACK outperform the AACK schemes by approximately 3%; (iv) The packet delivery ratio of AACK and TWOACK schemes is almost the same; (v) The routing over head in case of A3ACK scheme is almost the same as in case of AACK scheme which in average is less than the routing over head for the TWOACK scheme, and (vii) The average of the packet delivery ratio is 93% and the average of the routing over head is 12%.

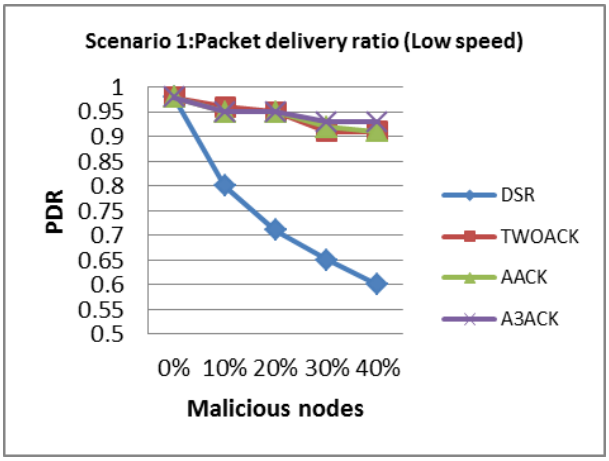

Fig 8: Result of PDR for low speed in scenario 1

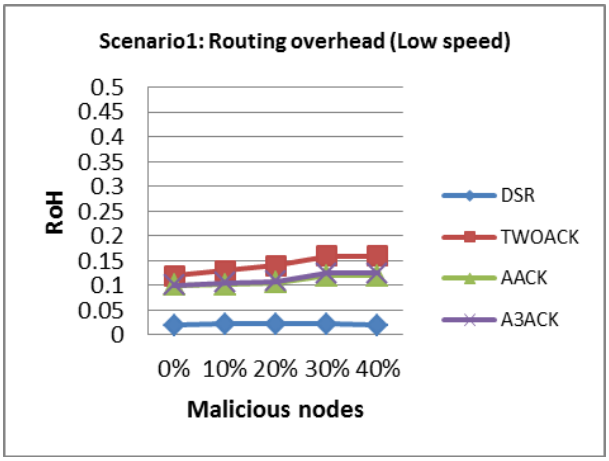

Fig 9: Result of RoH for low speed in scenario 1

6.2 Results of Scenario 1 with High-Speed Mobility

Total Dropping: (i) Generally in high mobility the routing overhead increases in ACK based IDS from the case of low mobility by around 10%; thereby, it is larger than the overhead of Watchdog and DSR by around 25% .while the enhancement in the performance, i.e. PDR, is about 10%; (ii) For packet delivery ratio metric in the presence of small number of malicious nodes, the AACK outperforms the TWOACK by approximately 15% , but in case of large number of malicious nodes the TWOACK outperform the AACK because of the switching overhead of AACK, and (iii) The packet delivery ratio of AACK and A3ACKs schemes is almost the same.

Partial Dropping (50%); as shown in Figure 10 and Figure 11: (i) Generally in high mobility the routing overhead increases in ACK based IDS from the case of low mobility by around 15%; thereby, it is larger than the overhead of DSR by around 25% .while the enhancement in the performance, i.e. PDR, is about 15%; (ii) For packet delivery ratio metric in the presence of small number of malicious nodes, the AACK is the same as TWOACK , but in case of large number of malicious nodes the TWOACK outperform the AACK because of the switching overhead of AACK; (iii) The packet delivery ratio of AACK and A3ACKs schemes is almost the same with a slightly outperformance in the case of 30% and 40% malicious nodes, and (iv) The average of the packet delivery ratio is 67% and the average of the routing over head is 30%.

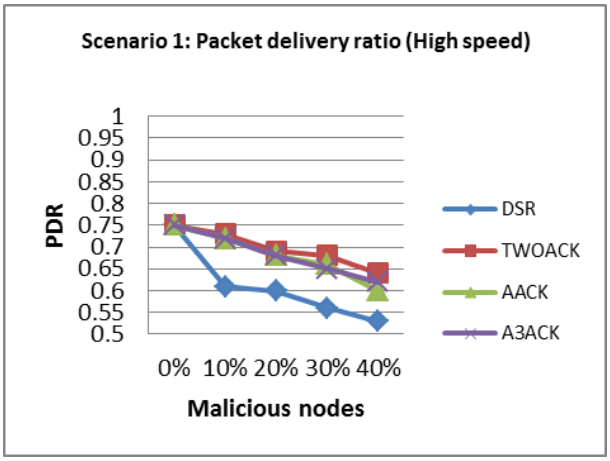

Fig 10: Result of PDR for high speed in scenario 1

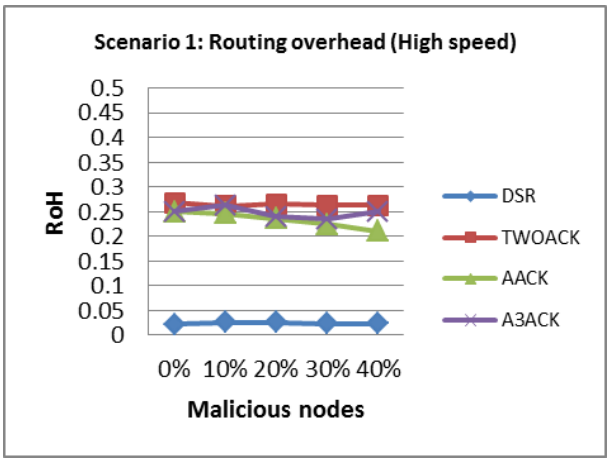

Fig 11: Result of RoH for high speed in scenario 1

6.3 Results of Scenario 2 with Low-Speed Mobility

Total Dropping: (i) A3ACK scheme slightly outperforms AACK scheme when the malicious nodes ratio is between 10% and 20%. However, A3ACK scheme surpasses AACK by about 10% and 13% when the malicious nodes ratio is between 30% and 40% respectively; (ii) Due to the stability in low speed network the packet delivery ratio for both A3ACK scheme and AACK scheme in low speed network is higher than that in high speed network, and (iii) Routing overhead for both A3ACK scheme and AACK scheme in low speed network is lower than that in high speed network due to stability in low speed network.

Partial Dropping (50%); as shown in Figure 12 and Figure13: (i) A3ACK scheme is the same as AACK scheme when the malicious nodes ratio is 10% and slightly outperform the AACK scheme when the malicious nodes ratio is 20%. However, A3ACK scheme surpasses AACK by about 9% and 8% when the malicious nodes ratio is between 30% and 40% respectively; (ii) Due to the stability in low speed network the packet delivery ratio for both A3ACK scheme and AACK scheme in low speed network is higher than that in high speed network; (iii) Routing overhead for both A3ACK scheme and AACK scheme in low speed network is lower than that in high speed network due to stability in low speed network, and (iv) The average of the packet delivery ratio 89% is and the average of the routing over head is 24%.

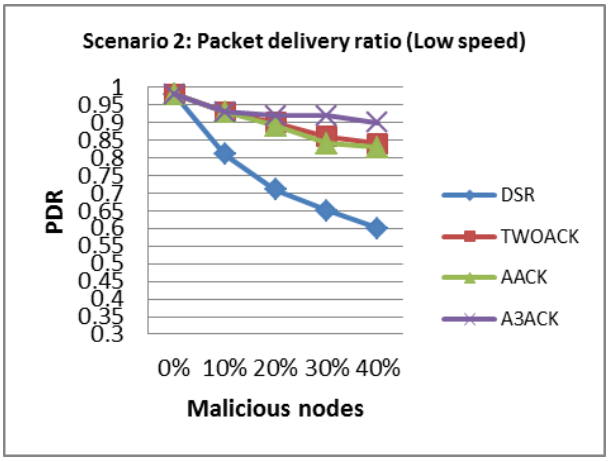

Fig 12: Result of PDR for low speed in scenario 2

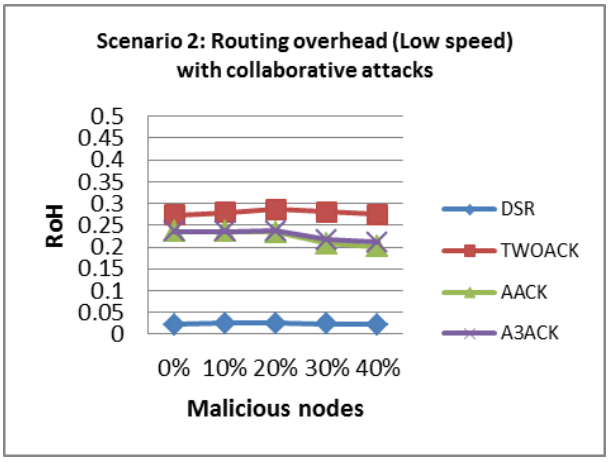

Fig 13: Result of RoH for low speed in scenario 2

6.4 Results of Scenario 2 with High-Speed Mobility

Total Dropping: (i) A3ACK scheme slightly outperforms AACK scheme when the malicious nodes ratio is between 10% and 20%. However, A3ACK scheme surpasses AACK by about 11% and 16% when the malicious nodes ratio is between 30% and 40% respectively and (ii) Routing overhead for A3ACK scheme is higher than AACK scheme especially at 40% MN.

Partial Dropping (50%); as shown in Figure 14 and Figure 15: (i) A3ACK scheme slightly outperforms AACK scheme when the malicious nodes ratio is between 10% and 20%. However, A3ACK scheme surpasses AACK by about 5% and 2% when the malicious nodes ratio is between 30% and 40% respectively and (ii) The average of the packet delivery ratio is 53% and the average of the routing over head is 24% which is not acceptable.

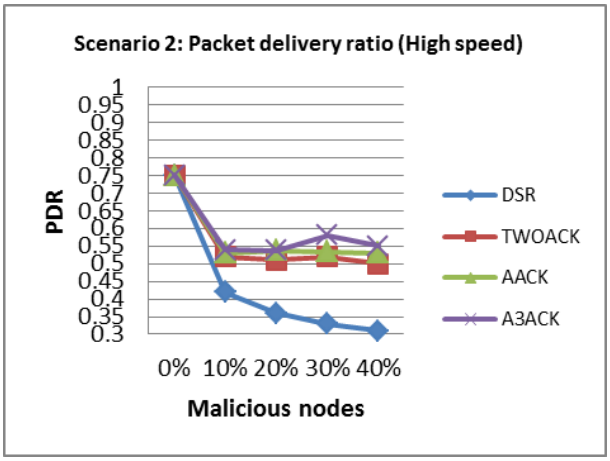

Fig 14: Result of PDR for high speed in scenario 2

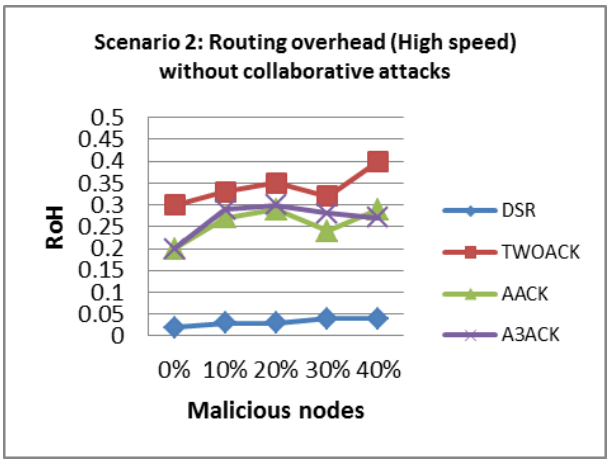

Fig 15: Result of RoH for high speed in scenario 2

7. CONCLUSION

In this paper, a discussion of a major drawback in watchdog technique is done which is its ability to detect dropping in the presence of partial dropping. This paper introduces an evaluation of the ACK based IDS techniques for dropping attack (partial dropping 50%) in MANETs using OMNET++ simulator to see if this kind of IDS techniques can actually overcome this major drawback in watchdog technique. From the discussion of the previous results with total dropping and the new result with partial dropping introduced by this research a similarity of the characteristics of curves with few changes is present. But the performance of the intrusion detection systems is actually improved in scenario 1 whether with low speed or with high speed. However, the performance of the intrusion detection systems decreases in scenario 1 with low speed by an average of 6% and decreases significantly with high speed by an average of 20%. From that, it is safe to say that this research proves that with high speed, the presence of collaborative attacks and partial dropping the ACK based techniques have low performance. But with the low speed the performance is acceptable.

8. REFERENCES

[1] Y. Kim, R.G. Evans, and W.M. Iversen, "Remote sensing and control of an irrigation system using a distributed wireless sensor network," IEEE Transactions on Instrumentation and Measurement, Vol.57, No.7, pp: 1379-1387, 2008.

[2] A.R. Kumar, M.K. Abhishek, et al., "A Review on Intrusion Detection Systems in MANET," International Journal of Engineering Science and Innovative Technology, Vol.2, pp: 609-618, March 2013.

[3] T. Anantvalee and J. Wu, "A survey on intrusion detection in mobile ad hoc networks," Springer US on Wireless Network Security, pp: 159-180, 2007.

[4] S. Marti, T.J. Giuli, K. Lai, M. and Baker, "Mitigating routing misbehavior in mobile ad hoc networks," Proceedings of the 6th annual international conference on Mobile computing and networking, 2000.

[5] N. Nasser and Y. Chen, "Enhanced intrusion detection system for discovering malicious nodes in mobile ad hoc networks," IEEE International Conference on Communications, 2007.

[6] D. Johnson, Y. Hu, and D. Maltz, "The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4". No.RFC 4728, 2007.

[7] A. Musaddiq and F. Hashim, "Multi-hop wireless network modelling using OMNET++ simulator," Computer, Communications, and Control Technology (I4CT) International Conference, pp: 559-564, 2015.

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

[9] K. Balakrishnan, J. Deng, and P.K. Varshney, "TWOACK: preventing selfishness in mobile ad hoc networks," Wireless communications and networking conference, Vol.4, pp: 2137-2142, 2005.

[10] A. Al-Roubaiey, T. Sheltami, A. Mahmoud, E. Shakshuki, and H. Mouftah, "AACK: adaptive acknowledgment intrusion detection for MANET with node detection enhancement," 24th IEEE International Conference on Advanced Information Networking and Applications, 2010.

[11] A. Basabaa, T. Sheltami, and E. Shakshuki, "Implementation of A3ACKs intrusion detection system under various mobility speeds," Procedia Computer Science, Vol.32, pp: 571-578, 2014.

[12] A. Varga and R. Hornig, "An overview of the OMNeT++ simulation environment," Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008.

[13] J. Broch, D.A. Maltz, D.B. Johnson, Y.C. Hu, and J. Jetcheva, ''A performance comparison of multi-hop wireless ad hoc network routing protocols," In Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking, pp: 85-97, 1998.