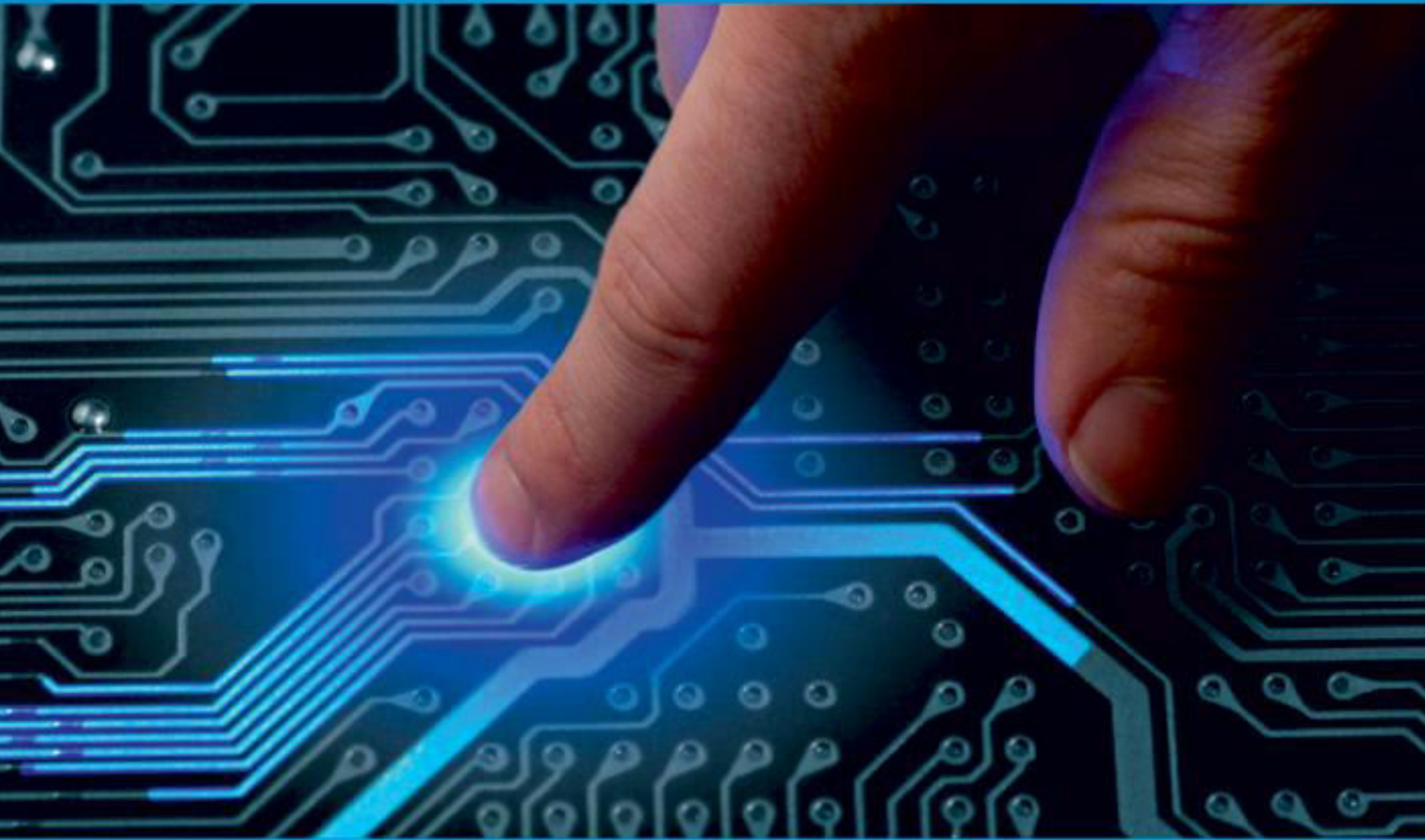
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 2, February 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

Packet Dropping Attack Based Detection Nodes in MANET

R.MOHANKUMAR, PRADEEP T

Assistant Professor, Department of Computer Applications (MCA), K.S.R. College of Engineering (Autonomous), Tiruchengode, India

Department of Computer Applications (MCA), K.S.R. College of Engineering (Autonomous), Tiruchengode, India

ABSTRACT: Mobile Ad hoc Networks (MANETs) is a kind of network composed of mobile devices distributed in a geographic area where there is a lack of fixed infrastructure or centralized administration. Nodes within communication range communicate directly, while those out of range make use of other nodes to forward the message to given destination. In MANETs packet dropping attacks have remarkable consequences among other threats. Malicious nodes drop received data or control messages instead of relaying them, thus by affecting the traffic in the network. Blackhole attacks imply malicious nodes dropping all the packets they receive. Grayhole attacks are similar but malicious nodes drop packets statistically by following a predetermined probability distribution. It should be emphasized that recognizing the actual cause(mobility, collision, errors, malicious behavior)for packet dropping in MANETs is still an open challenge, which is necessarily be addressed in order to reduce the number of false positives in IDS schemes. An Analytical model is introduced in order to distinguish between the legitimate packet dropping and malicious packet dropping behaviors. For that an enhanced windowing method is used for collecting the features from the network. From the features, the probabilities are to be calculated that are involved in analytical model. Based on the dropping probability that is estimated, concluded that the analyzed packet dropping node is malicious or legitimate by comparing with the predefined detection threshold.

KEYWORDS: Malicious node, packet dropping attack, Event based windowing method, MANETs

I.INTRODUCTION

1.1 Overview of MANETs

Ad hoc networks form spontaneously without a need of an infrastructure or centralized controller. This type of peer-to-peer system infers that each node, or user, in the network can act as a data endpoint or intermediate repeater. Thus, all users work together to improve the reliability of network communications. These types of networks are also popularly known to as mesh networks because the topology of network communications resembles a mesh. Mobile applications present additional challenges for mesh networks as changes to the network topology are swift and widespread. Such scenarios require the use of MANET technology to ensure communication routes are updated quickly and accurately. MANETs are self-forming, self-maintained, and self-healing, allowing for extreme network flexibility. While MANETs can be completely self contained, they can also be tied to an IP-based global or local network. MANET is a self-configuring network of mobile routers connected by wireless links the union of which form a random topology. The routers are free to move randomly and organize themselves, thus the network wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural or human-induced disasters, military conflicts, emergency medical situations etc.

1.2 RTS AND CTS MECHANISM

According to this mechanism before actual data transfer, sender and receiver exchange RTS/CTS packets to reserve the channel for data transmission. It is also called virtual carrier sensing because in this mechanism nodes get the information about the state of channel by exchanging a pair of control packets, rather than sensing the channel physically. In Figure 1.1 node A has data to send to node B, it first sends RTS packet to node B in which node A fills the address of node B and time required to complete data transmission. On receiving RTS packet from node A, node B replies with CTS packets. The RTS of A is also received by node C because node C is also in transmission range of A. Node C determines that it is not the intended receiver so it blocks itself from accessing the channel by setting a timer known as Network Allocation Vector (NAV). During this blocking state node C can neither start any data transmission nor reply to any RTS packet of any other node in its neighbourhood. D is a node that is in transmission range of node B and receives the CTS packet of B. So D will also set a NAV timer to prevent any data transmission during the transmission of data from node A to node B. NAV is a counter that decreases constantly and initialized to a value stored in RTS or CTS packet. The timer set by node C is called RTS NAV timer and the timer set by node D is called CTS NAV timer. Now node A starts actual data transmission to B. After receiving the complete data accurately, node B replies with acknowledgement ACK packet to indicate the success of transmission. The RTS/CTS mechanism informs all stations in the range of the sender and the access point (receiver) about the planned transmission and instructs them not to send for the reserved duration. Thus it serves two purposes: Since the RTS and CTS packets are short, a collision will only last for the duration of the short packet. The following data and ACK packets are transmitted without collision.The hidden station problem can be avoided, since all stations in the range of the receiver are informed about the transmission and wait until it is finished

.

1.3 Types of attacks in manets

Black hole attack

In black hole attack, the sender node receive reply message from fault node and make smallest way to receiver node. Fault node sends reply message after authorised node to sender node and then sender become confuse in two replies. On that way, Fault node become sender node and whole data received by it. In this, the data packets are fully dropped.

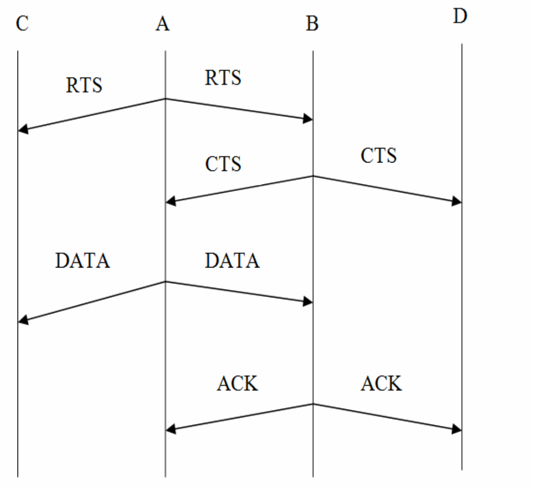


Figure 1.1 RTS and CTS Mechanism

1.Gray hole attack

Grey hole attack is a node which react maliciously for some specific time duration by releasing packets but may come to balanced behaviour and later forward the packets through packet ID to other packet. A Grey hole may also behave a random behaviour by which it rejects some the packets randomly when it forward to other packets. Thereby its detection is even more difficult than black hole attack.

II. RELATED WORK

Djenouri D, Badache N et al (2005) proposed 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehavior and to mitigate their adverse effect. The main idea of the 2ACK scheme is to send two-hop acknowledgement packets in opposite direction of the routing path. In order to reduce additional routing overhead, only a fraction of the received data packets are acknowledged in the 2ACK scheme. The 2ACK technique is based on a simple 2-hop acknowledgment packet that is sent back by the receiver of the next-hop link. Compared with other approaches the 2ACK scheme overcomes several problems including ambiguous collisions, receiver collisions and limited transmission powers.

Basile C, Kalbarczyk Z T, Iyer R K et al (2007) evaluates strategies to build reliable and secure wireless ad hoc networks. It is based on the notion of inner circle consistency, where local node interaction is used to neutralize errors or attacks at the source, both preventing errors from propagating in the network and improving the fidelity of the propagated information. Thus an unreliable and insecure wireless network is transformed into dependable network substrate on top of which application benefilt from improved network reliability and security. This is achieved by combining statistical and threshold cryptography techniques with application aware checks to exploit the data or computation that is partially and naturally replicated in wireless application.

Tamilselvan L, Sankaranarayanan V,et al (2008) proposed a fidelity table where in every participating node will be assigned a fidelity level that acts as a measure of reliability of that node. In case the level of any node drops to 0 it is considered to be malicious node, termed as black hole and is eliminated. The black hole attack can be easily deployed against the MANET and a feasible solution is provided by making use of fidelity tables and assigning fidelity levels to the participating nodes. The percentage of packets received through the proposed approach is better than that in AODV in presence of co-operative black hole attack.

Djahel S, Nait-abdesselam F, Zhang Z, et al (2011) presented two techniques that improve throughput in an ad hoc network in the presence of nodes that agree to forward packets but fail to do so. To mitigate this problem, the nodes are categorized based upon their dynamically measured behavior.Watchdog that identifies misbehaving nodes and a pathrater that helps routing protocols avoid these nodes. Through simulation watchdog and pathrater using packet throughput, percentage of overhead transmissions and the accuracy of misbehaving node detection. By the analysis of two techniques increases throughput in a network with moderate mobility and the benefits of an increased number of routing nodes while minimizing the effects of misbehaving nodes.

Baadache A, Belmehdi A, et al (2012) developed an approach to verify the correct forwarding of packets by an intermediate nodes. The Merkle Tree principle has been used for implementation in justification of proposed approach. Packet forwarding in multi-hop wireless ad hoc network is a co-operative task in which intermediate nodes participate voluntarily to deliver the packets to the destination node. An intermediate node can behave selfishly or maliciously to drop packets going through it, instead of forwarding them to its successor. This misbehaving can be called packet dropping attack as its main motivation is to prevent its resources like its limited energy or launch of denial of service attack. To avoid this the proposed scheme consist of need of acknowledgment for the reception of packets of the intermediate nodes. Using this, the source node constructs Merkle tree and compares the value of the tree root with the precalculated value. If both value are equal then the end-to-end path is free from packet dropper. Thus the approach has best delivery ratio and highest detection ratio.

III.PROPOSED WORK

3.1 Forwarding Process in MANETs

Forwarding process in MANET is modeled to develop our approach for dropping attack detection. The model considers different legitimate circum-stances in communications (collisions, channel errors or mobility) as well as malicious behaviors, and allows inferring how they all may affect the performance of the overall retransmission procedure.. After a data packet is correctly received by a node, several successive events must necessarily occur for the packet to be forwarded.

- Dest event: The considered node is not the final destination of the packet
- Rout event: The node has a valid route for relaying the packet towards the desired destination
- Drop event: The node is not a malicious dropper and, thus, it would not drop the packets instead of forwarding

them

If all of the previous events occur, the node tries to forward the packet. To do this, two subsequent actions are taken. First, the node will try to send a RTS message. This event is termed as RTS event, and its associated probability P_{RTS}. To estimate P_{RTS}, the above events are considered, there exists a route for the destination and the node is neither the final destination nor a dropper. Thus, P_{RTS} is computed as follows:

$$P_{RTS} = \Pr(RTS \mid dest, route) = (1\text{-}P_{DROP}) \qquad (4.1)$$

Where P_{DROP} is the probability that the packet is maliciously discarded by the node. Note that the event drop is modeled as a probability, meanwhile the events dest and rout are not. Since these two conditions could be easily determined by the inspection of every received packet in a node, in the calculation of the conditional probability given in equation (4.1) only consider those packets that fulfill the conditions dest and rout.Second, the node checks if it receives a CTS message. This message is received from the next hop in the route when the corresponding RTS packet has reached its destination and the CTS packet is successfully received. Let us term this as CTS event, and P_{CTS} its associated probability.RTS and CTS packets after being sent can be lost due to several legitimate reasons, RTS and CTS messages might suffer a collision if another node in the range of the receiver node transmits an RTS at the same time that the first RTS or CTS are sent. In addition, both messages may also be affected by channel errors, which prevent them from reaching their destination. Another scenario where a packet is discarded happens when the nodes are out of the communication range because they have moved and they did not have enough time to properly update the routing table. This way, they cannot communicate each other. All these circumstances cause messages to be lost and CTS packets not to be received, thus leading to an RTS retransmission. The IEEE 802.11 RTS/CTS procedure allows a limit number of attempts to retransmit RTS packets, if a sender does not receive any CTS reply in response to multiple retransmissions of an RTS packet up to a predefined limit, the sending process fails. This upper value is called Short Retry Limit (SRL), and its default value is 7. Once the SRL is exceeded, the corresponding packet is discarded, and the sender node assumes the link to be broken and the next hop to be no longer accessible. Therefore, the probability that the CTS message is correctly received at the sender node (CTS event) can be approximated as follows. The model divides this probability, P_{CTS}, in two terms. The first one is related to collisions or channel errors, taking into account those situations in which RTS retransmissions occur without exceeding the SRL limit. The second term is associated with mobility situations in which the number of RTS retransmissions is higher than SRL, thus considering the link as broken. Therefore, the CTS packet will be received if none of the two aforementioned situations happens. Thus, the probability that CTS event happens given that RTS event has occurred is as follows:

$$P_{CTS} = \Pr(CTS \mid RTS) = 1\text{-} (P_{COL} + P_{MOB}) \qquad (4.2)$$

where P_{COL} is the probability for the RTS or CTS packets to be lost due to collisions or channel errors, and P_{MOB} the probability of packets losses due to broken links caused by mobility circumstances. Finally, if the sender node captures the medium, it transmits the desired data, the data packet is forwarded by the node (FWD event). To forward the message, both the events RTS and CTS need to have occurred successfully, so the probability for the whole forwarding process, P_{FWD}, is computed as follows:

$$\begin{aligned} P_{FWD} &= \Pr(CTS.RTS \mid dest, rout) \\ &= \Pr(CTS \mid RTS) \,.\, \Pr(RTS \mid dest, rout) \\ &= (1\text{-} P_{DROP}) \,.\, [1 - (P_{COL} + P_{MOB})] \qquad (4.3) \end{aligned}$$

3.2 Event based windowing method

A normal methodology is to monitor these features by considering temporal observations over successive non-overlapped analysis windows of fixed duration. However, this methodology presents two main drawbacks.

The first one is related to situations where the temporal window ends just after the transmission of an RTS packet. Here, it is not possible to guess if the packet will be properly replied, if a collision will occur or if a mobility situation will happen. This fact can lead to undesirable effects due to the discontinuities caused by the windowing. In the Figure 4.2, dotted lines represent the end of the time windows. As it can be seen, the temporal window could end during the retransmission of an RTS, just after RTS #5 is sent. In this case, the whole circumstance which characterizes a mobility related situation will not be caught in any of the temporal windows, and therefore, the legitimate drops due to mobility will not be considered as legitimate, because mobility will not be detected.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165|

|| Volume 11, Issue 2, February 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1102010 |

The second drawback is related to the fact that, even if during a certain interval there are no features to collect or there are few, they will be analyzed anyway, thus obtaining biased information that could lead to wrong detection results. Suppose that in the temporal window only few data packets are received or just one is. Suppose that the temporal window ends even before the CTS in response to RTS #1 is received too. In such a case, the analytical model will consider a very high percentage of dropped packets thus leading to the misclassification of the node as malicious. To overcome these inconveniences, an event-based windowing procedure is used instead of a time-based one. The features are obtained for non-overlapping windows of P received data packets for each node in the network by event based windowing method. Examples of the differences between both types of windowing are shown in Figure 4.1 and 4.2, where dashed lines correspond to the end of the event windows. With event-based windows, the first problem is avoided, since the end of each window will always coincide with a data packet reception event. In Figure 4.1 evidences that, by employing the event-based windowing, that mobility situations can be fully collected. Either if the collection is performed after *DATA #x* is received or if it is performed when the node receives *DATA #x* + 1*,* the whole event is collected.Regarding the second problem now the collection of statistics will always consider the same number of events, *P*, thus attenuating the effect of biased information. In Figure 4.2 illustrates how our event-based scheme guarantees that a representative amount of data are used, thus minimizing potential wrong classifications. Besides the solution of these reported problems, an additional significant advantage should be mentioned for the proposed event-based windowing scheme. It refers to the fact that, if a given node is not receiving traffic at all, it makes no sense to perform a detection process every certain time, as this only involves a waste of the resources of the node. Thus, the use of the proposed windowing implies resources saving in nodes with scarce activity, since the detection procedure is expected to be launched fewer times, involving lower computation and, consequently, lower energy consumption.

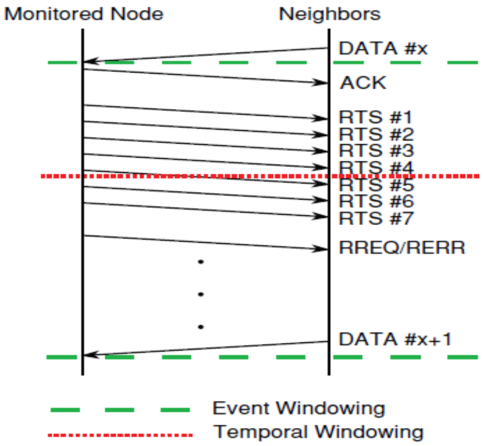


Figure 4.1 Discountinuties by time-based

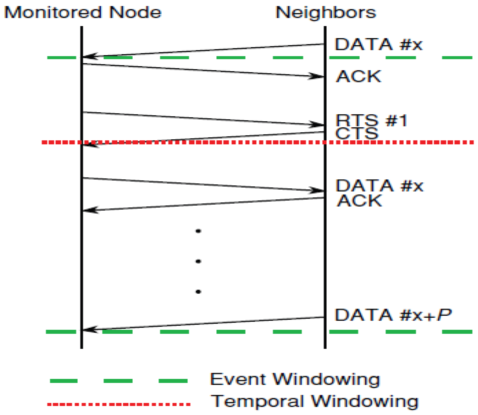


Figure 4.2 Biased information due windowing to time-based windowing

3.3 Detection Process

The features needed for the detection process are obtained from event based windowing method. The list of features obtained are:

- $\#RTS_{SENT,i}$: Total number of RTS messages sent by node N_i
- $\#CTS_{RECV,i}$: Total number of CTS messages sent by node N_i
- $\#DATA_{FWD,i}$: Total number of data packets forwarded by node N_i
- $\#DATA_{RECV,i}$: Total number of data packets received by node N_i
- $RREQ_i$: A boolean feature whose value is true if RREQ message has been broadcasted by node N_i, and otherwise FALSE

Calculation of Probabilities

The parameters to be estimated are P_{FWD}, P_{COL} and P_{MOB}. An empirical approximation is going to be used to estimate both P_{FWD} and P_{COL}. First, P_{FWD} can be calculated as the percentage of data packets forwarded by the node with regard to the number of packets received by it. With this purpose, the traffic of the analyzed node in search of received data packets whose destination is not the analyzed node itself. The estimator for this probability, P_{FWD}, is as follows:

$$P_{FWD} = \frac{\#DATA_{FWD}}{\#DATA_{RECV}} \qquad (4.4)$$

It must be reminded that, only if a node is not the final destination of the packet and there exists a valid route, the packet will be counted as a received data packet in $\#DATA_{RECV}$ .About the legitimate packet discards, our model distinguishes two possible situations: (i) the one happening due to collisions or channel errors, which takes into consideration those RTS retransmissions not exceeding the SRL value and contributes to P_{COL} and (ii) the situation contributing to P_{MOB}, which is caused by broken links and considers those RTS retransmission exceeding the SRL value. Regarding P_{COL}, since the associated effect is related to the traffic load, the number of RTS packets sent by the node without a proper CTS reply ($\#RTS_{SENT} - \#CTS_{RECV}$) is computed, as well as the total number of attempts to seize the channel.The packets which are not directly related to broken links situations are taken into account, those RTS retransmissions which do not exceed the SRL limit. An estimator for the collision and channel error probability, P_{COL}, can be computed as follows:

$$P_{COL} = \frac{\#RTS_{SENT} - \#CTS_{RECV}}{\#RTS_{SENT}} \qquad (4.5)$$

The proposed estimator for the probability of a broken link situation can be easily computed, it will take one of just two values. P_{MOB} is set to 1 when the number of RTS retransmissions exceeds the SRL limit in a measuring window, since here the node considers that it does not have a connection with the next hop. The estimator is set to 0 otherwise, because the link is not considered to be down. That is,

$$P_{MOB} = \begin{cases} 1, & \text{if } \#RTS_{SENT} \geq SRL \\ 0, & otherwise \end{cases} \qquad (4.6)$$

Taking into account of all above facts and considering all features the probability of dropping is calculated. The dropping probability which decides the analyzed node is malicious or not. The probability of occurrence of packet dropping can be calculated as follows:

$$P_{DROP} = \begin{cases} 0, & \text{if } P_{MOB} = 1 \\ 1 - \frac{P_{FWD}}{1 - P_{COL}}, & \text{otherwise} \end{cases} \qquad (4.7)$$

This dropping probability is subsequently compared to a predefined detection threshold θ (θ = 0.15). If P_{DROP} is greater than this threshold and according to an anomaly based approach, it is concluded that the analyzed node is malicious, and legitimate otherwise.

IV. RESULT AND DISCUSSION

The detection performance of the introduced IDS is evaluated by means of two well known parameters, namely the True Positives Rate (TPR), or detection accuracy/rate, and the False Positives Rate (FPR). As known, we obtain a number of operating points to estimate the Relative Operation Characteristic (ROC) curve by varying the decision threshold θ. It is important to note that the ROC curve has been obtained by repeating 75 times . The maximum speed of the nodes is set to 10 m/s in all the cases. This way, our results are comprised of the mean value of these 75 simulations and the 95% confidence intervals of these averages.The ROC curves obtained for both stand-alone and distributed implementations. As expected, the results obtained for the distributed-collection IDS approach are a little bit worse than the ones got in the stand-alone case. This is due to the fact that, in the distributed case, an approximation for two features is used, which considers that every sent CTS and data packet will be received. As a very little portion of these packets can be lost due to channel errors or collisions, the performance of this scheme is slightly deteriorated. As shown in the curve, FPR improves and TPR decreases as the detection threshold θ increases. On the contrary, lower detection thresholds result in better TPR values, but in in-creasing FPR figures. This is coherent with the fact that upper (lower) values for the detection threshold imply lower (up-per) sensitivity of the system against “malicious” behaviors. Of course, in such a case the FPR (TPR) values are improved. The optimal operating point of the system is achieved empirically from the above results. In particular, θ (which must be in the range [0−1], as it is compared to a probability value) is set to 0.15, as it seems to represent a good tradeoff between FPR and TPR.

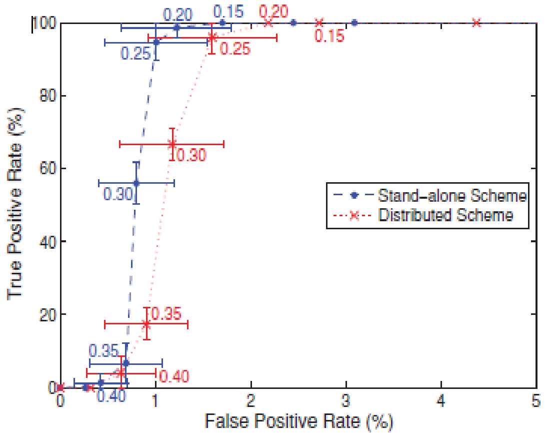


Fig 4.1 ROC curve for standalone and distributed implementations by varying the parameter

V. CONCLUSION AND FUTURE WORK

Proposed analytical model is intended to detect malicious packet dropping behaviors in Mobile Ad hoc Networks. An event based windowing procedure for features collection and subsequent analysis process is proposed. It eliminates some limitations of normal time-based windowing method and is able to improve the performance in nodes which exhibit low or null activity, resulting in lower consumption of resources. As future work this project can be further enchansed to include an attack model where several nodes work in collusion to evade the detection process.

REFERENCES

1. Baadache A, Belmehdi A,(2012) ‘Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks’, Journal of networks; pp.1130-1139.
2. Basile C, Kalbarczyk Z T, Iyer R K,(2007) ‘Inner Circle consistency for wireless ad hoc networks’, IEEE Trans, Mobile computing; pp.39-55.
3. Djahel S, Nait-Abdesselam F, Khokhar A,(2011) ‘Mitigating packet dropping problem in mobile ad hoc networks: proposals and challenges, IEEE Commun; pp.658-672.

4. Djenouri D, Badache N, (2005) ‘New approach for selfish nodes detection in mobile ad hoc networks’, in: Proceedings of the Workshop on First International Conference on security and privacy for Emerging Areas in Communication Networks(SecurComm); pp.288-294.
5. Garcia-Teodoro P, Sanchez-Casado L, Macia-Fernandez G, (2014) ‘Taxonomy and holistic detection of security attacks in MANETs’, Security for Multihop Wireless Networks; pp. 1–12.
6. Hayajneh T, Krishnamurthy P, Tipper D, Kim T, (2009) ‘Detecting malicious packet dropping in presence of collisions and channel errors in wireless ad hoc networks’, in: Proceedings of the IEEE International Conference on Communications (ICC);pp.1-6.
7. Huang Y, Fan W, Lee W, Yu P S, (2003) ‘Cross-feature analysis for detecting ad- hoc routing anomalies’, in: Proceedings of the 23rd IEEE International Conference on Distributed Computing Systems (ICDCS); pp. 478–487.
8. Kurosawa S, Nakayama H, Kato N, Jamalipour A, Nemoto Y,(2007) ‘Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method’, Int. J. Netw. Secur;pp.338–346.
9. Leovigildo Sanchez C, Gabriel Macia F,Pedro Garcia T, Roberto Magan C,(2015) ‘A model of data forwarding in MANETs for lightweight detection of malicious packet dropping’, computer networks; pp.44-58.
10. Marti S, Giuli T, Lai K, Baker M, (2000) ‘Mitigating routing misbehavior in mobile ad hoc networks’, in: Proceedings of the sixth Annual International Conference on Mobile Computing and Networking (MobiCom); pp. 255–265.
11. Rappaport T, Annamalai A, Buehrer A M, Tranter H,(2002) ‘Wireless communications past events and a future perspective’, IEEE Communications;pp.8–161.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING