PLOS ONE

RESEARCH ARTICLE

FSM-F: Finite State Machine Based Framework for Denial of Service and Intrusion Detection in MANET

Malik N. Ahmed*, Abdul Hanan Abdullah, Omprakash Kaiwartya

Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru, 81310, Malaysia

* mali7k@gmail.com

Abstract

Due to the continuous advancements in wireless communication in terms of quality of communication and affordability of the technology, the application area of Mobile Adhoc Networks (MANETs) significantly growing particularly in military and disaster management. Considering the sensitivity of the application areas, security in terms of detection of Denial of Service (DoS) and intrusion has become prime concern in research and development in the area. The security systems suggested in the past has state recognition problem where the system is not able to accurately identify the actual state of the network nodes due to the absence of clear definition of states of the nodes. In this context, this paper proposes a framework based on Finite State Machine (FSM) for denial of service and intrusion detection in MANETs. In particular, an Interruption Detection system for Adhoc On-demand Distance Vector (ID-AODV) protocol is presented based on finite state machine. The packet dropping and sequence number attacks are closely investigated and detection systems for both types of attacks are designed. The major functional modules of ID-AODV includes network monitoring system, finite state machine and attack detection model. Simulations are carried out in network simulator NS-2 to evaluate the performance of the proposed framework. A comparative evaluation of the performance is also performed with the state-of-the-art techniques: RIDAN and AODV. The performance evaluations attest the benefits of proposed framework in terms of providing better security for denial of service and intrusion detection attacks.

Citation: N. Ahmed M, Abdullah AH, Kaiwartya O (2016) FSM-F: Finite State Machine Based Framework for Denial of Service and Intrusion Detection in MANET. PLoS ONE 11(6): e0156885. doi:10.1371/journal.pone.0156885

Editor: Yongtang Shi, Nankai University, CHINA

Received: December 25, 2015

Accepted: May 21, 2016

Published: June 10, 2016

Data Availability Statement: All relevant data are within the paper and its Supporting Information file.

Funding: The authors have no support or funding to report.

Competing Interests: The authors have declared that no competing interests exist.

Introduction

In recent times, intrusion detection systems for MANET have received considerable attention, as a result of the importance of this kind of networking in daily life, and this has coincided with increased attacks on them. Most of today's applications are real-time applications, which need to deliver data at the right time and with the use of available resources. Any activity in a computer system that violates the security or availability of resources can be classified as an intrusion [1]. Preventive and reactive approaches are applied by most security solutions, in order to

protect MANET's routing protocol, services and applications. Preventive schemes based on encryption algorithms and key management help prevent unauthorised actions from affecting normal MANET operations, but these schemes add additional load traffic to the already limited bandwidth and power of MANET [2]. Reactive security mechanisms serve as a second defence line that detect and stop attacks that have passed through the first defence line. An Intrusion Detection System (IDS) can be used as an effective reactive mechanism for detecting misuse and perversion. It statistically analyses the normal and abnormal behaviour of nodes, by collecting information from legitimate users over a period of time [3].

IDS is software is designed to provide monitoring systems for network activities, detecting if there are any suspicious activities or policy violations. It considered a second line of defense [4, 5], while it also generates a report about the situation of the network to the security system, in order to allow appropriate action to be taken against the detected attack. Traditional wired networks using Intrusion Detection (ID) algorithms are not suitable for MANETs, because of differences regarding their characteristics, structures and operations.

In the context of security challenges in dynamic network environment, in this paper, a framework based on Finite State Machine (FSM) is presented for denial of service and intrusion detection in MANETs. In particular, an Interruption Detection system for Adhoc On-demand Distance Vector (ID-AODV) protocol is presented based on finite state machine. The packet dropping is considered as denial of service attack and sequence number duplication is considered as intrusion attacks. Detection systems for both types of attacks are designed using the concept of FSM. The major functional modules of ID-AODV includes network monitoring system, finite state machine and attack detection model. The proposed framework is implemented in network simulator NS-2 for evaluating the performance individually and comparatively with the state-of-the-art technique: RIDAN [6] and AODV [7].

Rest of the paper is organized in following sections. Section 2 qualitatively reviews security techniques applied on AODV. A background knowledge of AODV and the security attacks is provided in section 3. Section 4 presents the details design of FSM based ID-AODV. Simulations and analysis of results are discussed in section 5. Finally, section 6 concludes this paper with some future directions of research in the area.

Related Works

There are many proposals regarding lightweight IDS, but they have mainly focused on accuracy sacrificing lightweight. They select more features from the collected audit data, as a means of realising accuracy, which may in turn increase the weight of the intrusion detection algorithm. Some of the proposed lightweight intrusion detection agents, such as that of Tokekar and Jain [8], collect audit data periodically within specific timeframes. To make the IDS lightweight, as a means of saving energy, this allows other nodes with available batteries to participate in intrusion detection. However periodic data collection is still a problem, making the IDS heavyweight. Mutly et al. and Xenakis et al. have proposed that distributed cooperative intrusion detection, involving the exchange of intrusion reports between detection engine nodes, can increase detection accuracy. However the additional communication overhead will result in significant decreases in network performance, making the intrusion detection algorithm heavyweight [9,10].

An adaptive problematic nodes method has been proposed by A. Nadeem et. al, to evaluate the performance of the internal link in localising malicious nodes and detecting faulty links [11]. The authors' claims that the proposed scheme beats the existing security approach for improving anomaly-based detection approaches, considering resource-constrained MANETs. They also claim that they are the first to introduce NT technology as a means of developing

intrusion detection and spatial-time monitoring for MANET. Therefore, generally ID algorithms are considered to be lightweight if they consume less energy. Kheyri et al., Nadeem et al., Joseph et al. and Damopoulos et al. have all proposed Intrusion Detection Systems as a means of detecting new and unknown attacks, while they can also detect attacks that try to exploit unforeseen vulnerabilities [12–15]. Their ID systems are classified as behavioural or anomaly-based detection systems. General false alarms and false positives are two well-known limitations of the Intrusion Detection Systems. Other limitations are correlated to this type of IDS, including exchanging models among nodes, and the periodic normal profile updates which add significant overhead communication and processing. Building the best knowledge database takes time and effort.

Other type of Intrusion Detection based on misuse or signature can detect known attacks and intrusive activities accurately, efficiency, and faster. There is no need for a model exchange or complex time-consuming computations [16–18]. Despite these advantages, the attack specifications data need to reserve space in memory this space may not be used. Other limitations it can detect unknown attacks and need a hard work to manage the attack signature, there is a problem in detecting ingenious attacks, in addition to false alarm. Based on the Timed Finite State Machine, Stamouli, Argyroudis and Tewari [6] has proposed a real time system for the AODV MANET routing protocol. They have used a knowledge-based method to build real time monitoring system architecture called Real-time Intrusion Detection for Ad hoc Networks (RIDAN). The proposed architecture works as an interface between the network layer and the link layer, countering attacks by lessening their effectiveness, and keeping network performance within acceptable levels. RIDAN does not employ any authentication technique, and therefore it cannot detect any attack that violates authentication.

AODV Routing Attack

AODV presents numerous opportunities for assailants. This study first identified various abuse objectives that an inside assailant may need to accomplish [19–21]. The abuse objectives might include one or more the following:

- Route Disruption: Route Disruption involves either breaking down a current course, or preventing another course from being secured.
- Route Invasion: Route intrusion implies that an inside assailant can include themselves into a course between two end-points within a corresponding channel.
- Node Isolation: Node disconnection refers to keeping a given hub from imparting with any other hub in the system. This contrasts with Route Disruption, in that Route Interruption focuses on a course with two given end-points, while hub disconnection covers all conceivable courses.
- Resource Consumption: This refers to consuming the correspondence data transmission within the system or storage rooms at individual hubs. For example an inside assailant may devour the system data transmission by shaping a circle in the system.
- Denial of Service.

To attain these objectives, the following abuse activities or assaults need be addressed.

Packet Dropping Attack

In a bundle dropping assault, the assailant essentially drops the packets. Bundle dropping can be identified through checking whether a neighbour advances parcels towards the last objective. In

order to have the capacity to do this, it is important to keep up a neighbour table. This assault might be partitioned into different subcategories. In the event that an assailant applies such assaults to all Route REQuest (RREQ) messages it obtains, this sort of abuse is comparable to not having the assaulted hub in the system. An inside assailant may additionally specifically drop RREQ messages. Aggressors that dispatch such abuses are by their nature comparable to narrow-minded hubs. In the event that the assailant applies this assault to a Route REPly (RREP) message, this can now and again result in course disturbance. The assault can be additionally connected to information parcels, through which an inside assailant keeps an exploited person hub from accepting information parcels from different hubs over a brief period of time. The assailant may make a number of alterations after it obtains a RREQ message from the exploited person hub, which can include increasing the RREQ ID by a small amount, replacing the goal IP address with a non-existent IP address, increasing the source grouping number by no less than one, and setting the source IP deliver in the IP header to a non-existent IP address. The aggressor then telecasts the manufactured message.

At the point when the assailant neighbours receive the faked RREQ message, they redesign the following jump from the source hub to the non-existent hub, since the faked RREQ message will have a more prominent source arrangement number. Because of the non-existent end IP address, the faked message could be telecasted to the most distant hubs of the commercial hoc system. At the point when different hubs need to send information bundles to the source hub, they will utilise the courses built by the faked RREQ message, and the information parcels will be dropped due to the non-existent hub. This assault, notwithstanding, cannot completely detach the victimised person hub due to neighbourhood repair instruments within the AODV convention. Alternate hubs will launch an alternate round of course disclosure, in the event that they notice that the information bundles cannot be conveyed effectively. Moreover, the victimised person hub may not even have the capacity to send information parcels to different hubs. A few nuclear abuses of RREQ messages use RREQ messages to include entrances to the steering table of different hubs. These sections are not the same as those secured through the ordinary trade of RREQ and RREP messages. Specifically, the lifetime of these sections relates to the default esteem, specifically four seconds as determined by this study's investigations. Subsequently, in order to make such passages successful, an aggressor needs to intermittently dispatch nuclear abuses.

Sequence Number Attack

The arrangement number demonstrates the freshness of courses to the related hub. An assailant conveys an AODV control parcel, which produces a substantial arrangement number of the exploited person hub, as it will change the course to that exploited person hub. The succession number could be expanded on in order to overhaul the other hubs' opposite course tables, or to diminish it as a means of stifling its redesign. This can apply to either the Source Sequence Number or the Destination Sequence Number. RREQ ID, alongside the source IP address, can effectively distinguish a RREQ message. It will show the freshness of a RREQ message. Since a hub acknowledges only the first duplicate of a RREQ message, an expanded RREQ ID alongside the source IP location can ensure that the faked RREQ message is acknowledged by different hubs.

Interruption Detection AODV (ID-AODV)

ID-AODV focuses on the State Transition Analysis Technique, which was first created in order to model host-based and system-based interruptions in a wired earth. Among all the directing conventions proposed for MANETs, AODV has been the most prevalent, and has turned into

an Internet standard. Additionally, this has been an explanation behind AODV becoming more and more helpless against assaults.

Outline of Interruption Detection AODV

This study's system focuses on the work presented by Stamouli et al. [6]. Like RIDAN, the system of Stamouli et al. utilises Finite State Machines to empower the continuous recognition of dynamic assaults. Additionally RIDAN does not offer an answer for conveyed structural planning, distinguishing assaults that require more than one-jump data. ID-AODV could be described as a building design model for interruption locations in remote Ad Hoc systems. This can be referred to as a structural planning model, on the grounds that it does not result in any changes to the underlying directing convention, but rather simply blocks steering and application activity. ID-AODV has been actualised on top of AODV, which has as of late become an internet standard. In any case, the assaults that ID-AODV intends to identify are particular to the AODV convention. The methodology of distinguishing assaults, and the general structural planning that might be reached out to work, has no overlap with different conventions like DSR. The framework takes after learning-based systems to catch system interruptions. The way that it utilises the Finite State Machine (FSM) empowers the framework to discover vindictive actions continuously, instead of utilising the factual examination of long ago caught activity. A limited state machine could be characterised as a dynamic machine comprised of a set of states, that include the introductory state, a set of information occasions, a set of yield occasions, and a state move capacity. The capacity takes the current state and an information occasion, and gives back when it is due a set of yield occasions and the following state. The state machine can additionally be seen as a capacity, serving to map a requested grouping of information occasions into a comparable arrangement of yield occasions. The interruption discovery part works mainly by taking an interest hub, and accordingly its execution relies on system activity. In view of the quantity of bundles obtained through whichever time unit, specifically through more than one FSM, there are some pieces of the interruption recognition part that may need to be activated. FSM was developed in the wake of concentrating on the inner operations of the AODV directing convention. In order to perceive the activity examples that occur when a pernicious assault takes place against the directing fabric, the convention's movement was dissected in terms of both its static and portable conditions. Fig 1 presents the top-level building design of ID-AODV.

Details of ID-AODV

This study will now present points of interest regarding the outlining and execution of the proposed ID-AODV. ID-AODV recognises assaults against the AODV directing convention through Wireless Mobile Ad Hoc Networks. The components of ID-AODV have been examined through the accompanying segments.

Network monitor (NM). The approach of Ad Hoc systems prevents any single IDS hub from watching all within a solicitation answer stream. Therefore, following RREQ and RREP messages, in an appeal answer stream must be performed through an appropriate system screen (NM). Fig 2 portrays the building design of a system screen. System screens latently listen to the ID-AODV steering message, and recognise wrong RREQ and RREP messages. Gathered messages focus on the appeal answer stream in which they have a place. An appeal answer stream might be interestingly recognised by the RREQ ID, including the source and end of the line IP addresses.

Finite state machine. Specification-based approaches provide a model for analysing attacks, based on protocol specifications. A detail-based methodology offers a model for examining

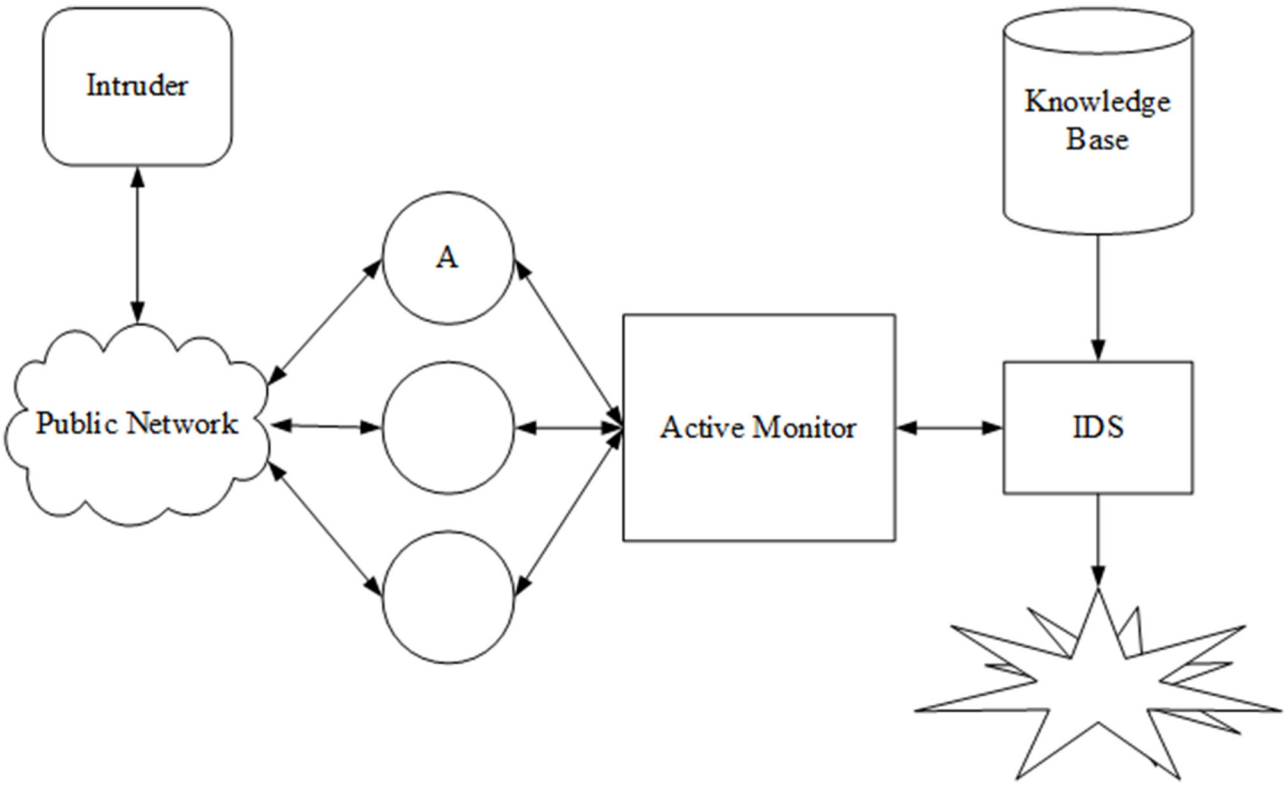

Fig 1. The Architecture of ID-AODV.

doi:10.1371/journal.pone.0156885.g001

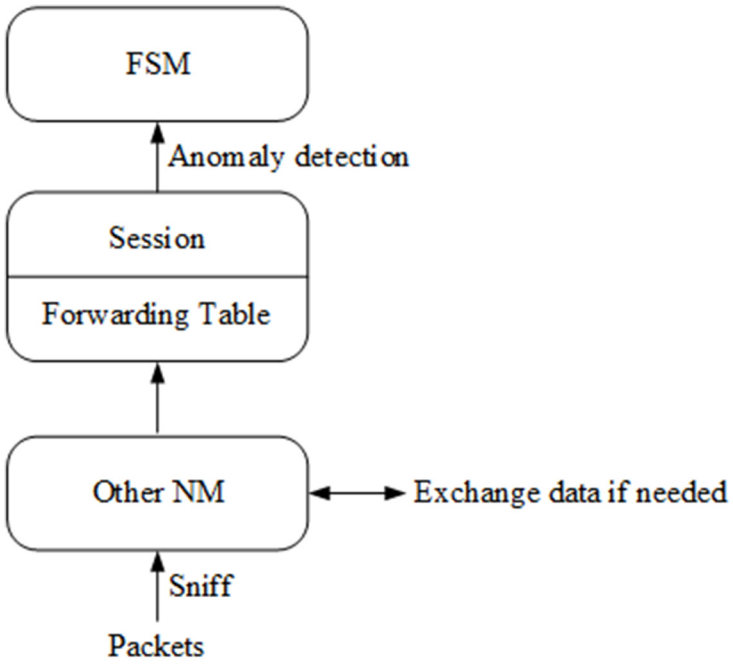

Fig 2. Network monitor.

doi:10.1371/journal.pone.0156885.g002

assaults with a focus on convention determinations. A system screen utilises a Finite State Machine (FSM) [18], in order to identify erroneous RREQ and RREP messages [6]. This maintains a FSM for each one extension of an appeal answer stream. An appeal stream begins at the 'Source' state. It travels to the 'RREQ Forwarding' state when a source hub shows the first RREQ message (with another REQ ID). At the point when a sent television RREQ is discovered, it stays in the 'RREQ Forwarding' state unless a comparable RREP is identified. At that point if a unicast RREP is recognised, it goes to the 'RREP Forwarding' state and stays there until it achieves the source hub and the course is situated up. In the event that any suspicious movement or peculiarity is distinguished, it goes to the 'Suspicious' or 'Alarm' states. At the point when a NM contrasts between another bundle and the old relating parcel, the essential objective of the demands is to verify that the AODV header of the sent control parcels has not changed in an undesired way. On the off chance that a middle of the road hub reacts to the appeal, the NM will confirm this reaction from its sending table, and additionally with the obligation to verify that the halfway hub is not lying. Furthermore, the stipulations are utilised in order to recognise bundle drop and caricaturing. Stamouli et al. [6] has not utilised system screens to follow RREQ and RREP messages in an appeal answer stream for the dispersed system. Meanwhile in the proposed FSM, this study has utilised the above streams.

Sequence number attack detection. In order for the interruption discovery to distinguish the succession number assault, this study dissected the RREQ and RREP messages. The research mimicked the assessment of IDS execution in both static and versatile conditions. The hubs identified as NM were static in both cases, in light of the fact that it is accepted that NM does not leave the allotted screen. New RREQ, for which the source hub is not enrolled in the neighbouring NM, sent RREP unicast by middle hub and no irregularity was identified. The IDS, following the diverse RREQ and RREP streams, started by the hubs. The IDS brought about postponing the course disclosure, due to including observing messages, and in addition to handling overhead in the checking hubs.

Analysis of Empirical Results and Discussion

In this section, implementation of the proposed IDS is carried out using network simulator NS-2. Network performance evaluation metrics including percentage of packet delivery ratio, percentage of false positive, percentage of detected bad nodes are utilized for analysing the performance of the proposed IDS. A comparative evaluation is also carried out with the state-of-the-art technique: RIDAN.

Simulation Environment

Simulations are carried out in maximum possible realistic network environment in a network simulator. A simulation area of size $1000 \times 1000m^2$ is considered for deploying mobile network nodes or hubs which uses random waypoint mobility model with the greatest seed set to 20 meters for every second. The stoppage time was considered as 15 seconds. An aggregate of 40 hubs were re-enacted and 16 of these hubs were imparting. Ten Constant Bit Rate (CBR) traffic associations were produced. Four hubs were hotspots for two streams in every case, and each of the two hubs were hotspots for a solitary stream. The end hubs received just one CBR stream each. IEEE 802.11 MAC layer model is utilized with the consideration of shared approach. The shadowing path loss radio propagation model with the radio range of 250m was considered. The packet drop timeout was set 10s and the packet drop threshold of 10 packets in a bundle was considered. The clear delay was set to 100 seconds as an occasion lapse clock. This was the measure of time through which a hub could be considered an occasion before touching base. Simulations were performed for over 900 seconds and results were noted down with an average

of 20 supination runs with same seed for the simulation. The aforementioned setting of parameters are summarized in Table 1.

Evaluation of Detection of Sequence Number Attack

The measurements utilized within the assessment of the 'sequence number attack' and the performance metric includes packet deliver ratio, falsely marked hubs and malicious node detection. For generating sequence number attack, duplicate packets with same sequence number were generated by source as well as intermediate sending hubs or nodes.

In Fig 3(a), impact of number of CBR connections on packet delivery ratio is presented under sequence number attack. It can be clearly observed that the packet delivery ratio of ID-AODV is higher as compared to the state-of-the-art techniques under sequence number attack. This can be attributed to the fact that the FSM based sequence number attack detection is better than the approach applied in the state-of-the-art techniques. In particular, packet delivery ratio of ID-AODV is in the range 49 – 71% whereas it is in the ranges 48 – 62% and 30 – 40% in case of RIDAN and AODV; respectively, under sequence number attack. In Fig 3(b), impact of average speed of nodes on packet delivery ratio is depicted under sequence number attack. The results clearly state that the packet delivery ratio of ID-AODV is higher in comparison with the state-of-the-art techniques under sequence number attack. This is because of better speed prediction and management of FSM based sequence number attack detection technique as compared to that of RIDAN. Due to the unavailability of speed prediction method in AODV, packet delivery ratio decreases with the increase in speed of nodes in the network. In particular, packet delivery ratio of ID-AODV is in the range 53 – 62% whereas it is in the ranges 51 – 60% and 35 – 50% in case of RIDAN and AODV; respectively, under sequence number attack.

In Fig 3(c), impact of percentage of malicious nodes on number of falsely marked hubs is depicted under sequence number attack. It is clear from the results that the number of falsely marked hubs is lesser in case of ID-AODV in comparison with those of the state-of-the-art techniques under sequence number attack. This is due to the better sequence number attack detection of FSM based technique. Due to the unavailability of sequence number attack detection method in AODV, number of falsely marked hubs increases with the increase in number of malicious nodes in the network. In particular, number of falsely marked hubs for ID-AODV is in the range 4 – 15% whereas it is in the ranges 8 – 20%and 25 – 39% in case of RIDAN and

Table 1. Basic setting of parameters in network simulator NS-2.

Parameter	Values
Simulation Area	$1000 \times 1000m^2$
Number of nodes or hubs	40
Packet size	512 Kbps
Traffic Type	CBR
Packet Timeout	10s
Packet Threshold	10 packets bundle
Delay	100s
Routing Protocol	AODV
MAC Protocol	IEEE 802.11
Mobility Model	Random Waypoint
Radio Propagation Model	Shadowing Path loss
Simulation Time	900s

doi:10.1371/journal.pone.0156885.t001

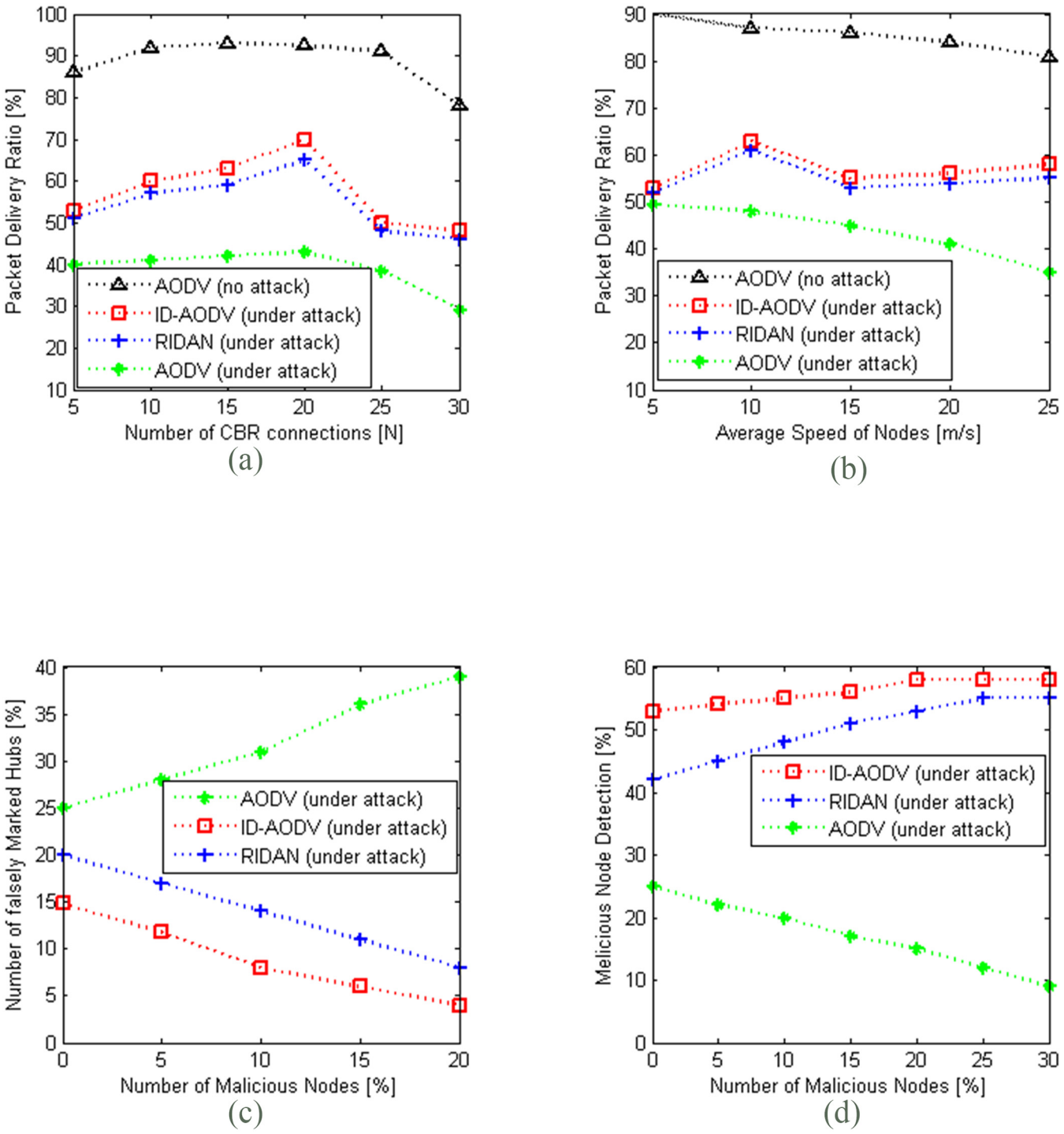

Fig 3. Under sequence number attack: (a) Impact of number of CBR connections on packet delivery ratio, (b) Impact of average speed of nodes on packet delivery ratio, (c) Impact of percentage of malicious nodes on number of falsely marked hubs, (d) Impact of percentage of malicious nodes on percentage of malicious node detection.

doi:10.1371/journal.pone.0156885.g003

AODV; respectively, under sequence number attack. In Fig 3(d), impact of percentage of malicious nodes on percentage of malicious node detection is shown under sequence number attack. It can be clearly observed that the percentage of malicious node detection is higher in case of ID-AODV as compared to those of the state-of-the-art techniques under sequence number attack. This can be attributed to the fact that the intrusion detection based on FSM in ID-AODV is qualitatively better than the approach applied in state-of-the-art techniques. Due to the unavailability of intrusion detection method in AODV, the percentage of malicious node detection decreases with the increase in number of malicious nodes in the network. In particular, the percentage of malicious node detection for ID-AODV is in the range 52 − 58% whereas it is in the ranges 42 − 55% and 25 − 9% in case of RIDAN and AODV; respectively, under sequence number attack.

Evaluation of Detection of Packet Dropping Attack

The evaluation of packet dropping attack detection is performed considering the metrics including packet deliver ratio, falsely marked hubs and malicious node detection. The packet dropping attack is generated deploying predefined intermediate nodes which do not establish communication with next hop nodes and drop the received packets intentionally. In Fig 4(a), impact of number of CBR connections on packet delivery ratio is presented under packet dropping attack. It can be clearly observed that the packet delivery ratio of ID-AODV is higher as compared to the state-of-the-art techniques under packet dropping attack. This can be attributed to the fact that the FSM based packet dropping attack detection is better than the approach applied in the state-of-the-art techniques. In particular, packet delivery ratio of ID-AODV is in the range 48 − 50% whereas it is in the ranges 35 − 47% and 20 − 21% in case of RIDAN and AODV; respectively, under packet dropping attack.

In Fig 4(b), impact of average speed of nodes on packet delivery ratio is depicted under packet dropping attack. The results clearly state that the packet delivery ratio of ID-AODV is higher in comparison with the state-of-the-art techniques under packet dropping attack. This is because of better speed prediction and management of FSM based sequence number attack detection technique of AI-AODV as compared to that of RIDAN. The packet delivery ratio decreases with the increase in speed of nodes in the network in case of AODV because of absence of speed prediction technique. In particular, packet delivery ratio of ID-AODV is in the range 31 − 50% whereas it is in the ranges 30 − 35% and 20 − 21% in case of RIDAN and AODV; respectively, under packet dropping attack. In Fig 4(c), impact of percentage of malicious nodes on number of falsely marked hubs is depicted under packet dropping attack. It is clear from the results that the number of falsely marked hubs in case of ID-AODV is lesser in comparison with those of the state-of-the-art techniques under packet dropping attack. This is due to the better packet dropping attack detection using FSM based technique in ID-AODV. Due to the unavailability of packet dropping attack detection method in AODV, number of falsely marked hubs increases with the increase in number of malicious nodes in the network. In particular, number of falsely marked hubs for ID-AODV is in the range 5 − 18% whereas it is in the ranges 13 − 25% and 32 − 55% in case of RIDAN and AODV; respectively, under packet dropping attack. These ranges are similar in nature but little bit higher than what were observed in case of sequence number attack in Fig 3(c). This is because of higher number of packet dropping nodes generated for the evaluation in this section.

In Fig 4(d), impact of percentage of malicious nodes on percentage of malicious node detection is shown under packet dropping attack. It can be clearly observed that the percentage of malicious node detection in case of ID-AODV is higher as compared to those of the state-of-the-art techniques under packet dropping attack. This can be attributed to the fact that the

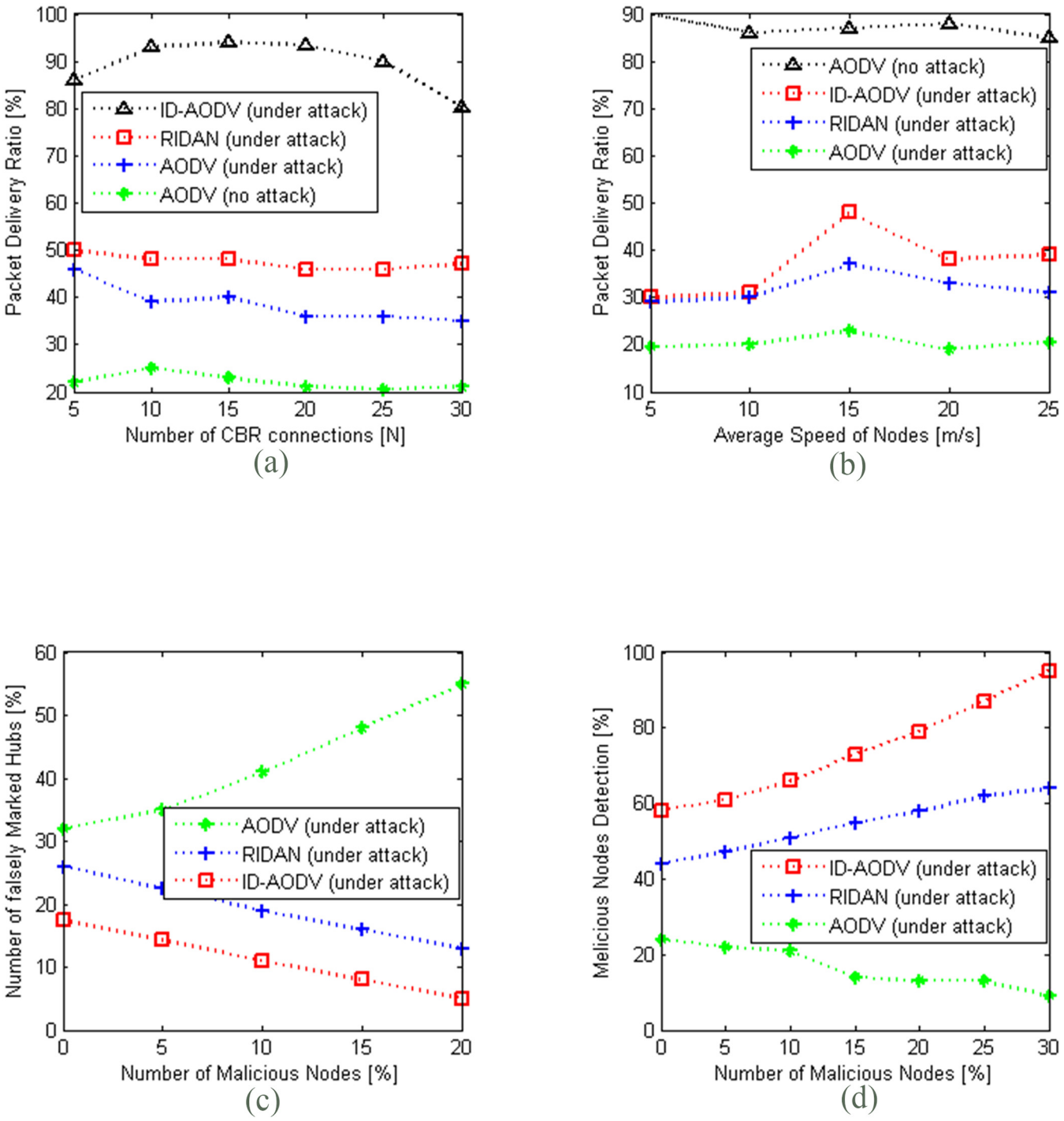

Fig 4. Under packet dropping attack: (a) Impact of number of CBR connections on packet delivery ratio, (b) Impact of average speed of nodes on packet delivery ratio, (c) Impact of percentage of malicious nodes on number of falsely marked hubs, (d) Impact of percentage of malicious nodes on malicious node detection.

doi:10.1371/journal.pone.0156885.g004

intrusion detection based on FSM in ID-AODV is qualitatively better than the approach applied in state-of-the-art techniques. Due to the unavailability of intrusion detection method in AODV, the percentage of malicious node detection decreases with the increase in number of malicious nodes in the network. In particular, the percentage of malicious node detection for ID-AODV is in the range 59 − 97% whereas it is in the ranges 43 − 63% and 22 − 8% in case of RIDAN and AODV; respectively, under packet dropping attack. These ranges are similar in nature but little bit higher than what were observed in case of sequence number attack in Fig 3 (d) of section 5.2 for ID-AODV and RIDAN but little bit lower for AODV. This is because of better detection rate with higher malicious nodes in ID-AODV and RIDAN in case of packet dropping attack.

Performance Comparison Analysis with RIDAN System

This section study presents the comparative consequences of this study's investigation and another study of RIDAN system by utilising the NS-2 test system for an Ad Hoc system, comprised of 40 hubs. The researchers expect that there is one gate crasher sending a grouping of sequential bundles, constituting an assault on the objective [22]. The interruption is considered to be recognised if the assault bundles pass through any of the hubs that constitute the interruption recognition framework. This study has utilised an arbitrarily chosen set of five out of 40 hubs, have explored different avenues presented by Stamouli et al. [6], and have considered a succession of five back to back parcels as constituting an assault signature. This study discovered the precision of identification both in regards to static and element conditions. It is not clear in Stamouli [6] how an assault requiring more than one-bounce data can be discovered, yet in ID-AODV multi-hop data is considered which beats the limit of the RIDAN framework. The researchers have created a rate of discovery of assault, utilising the RIDAN framework [6] for both static and element hub cases, which were not introduced in the earlier part of the work, and have also provided a relative execution of the ID-AODV and RIDAN frameworks underneath.

For the static case. This case considers that there is only one hub in the interruption recognition framework, arbitrarily chosen to be one hub out of 40. This study considers a framework in which the hubs constituting the interruption identification framework are picked haphazardly. This demonstrates the results of frameworks with the number of nodes set at 40 considering static case where nodes mobility is kept lower. In Fig 5, a comparison of impact of percentage of malicious nodes on interruption detection between the proposed ID-AODV and RIDAN systems is presented for the static case. It can be clearly observed that the performance of the proposed system is better as compared the state-of-the-art system. This can be attributed to the higher precision in terms of interruption detection of FSM based proposed system. Specifically, with 60% malicious nodes the proposed ID-AODV system is able to detect 99% of malicious nodes where RIDAN systems is able to detect 91% of malicious nodes. RIDAN system is able to detect 99% of malicious nodes only when the percentage of malicious nodes reaches to above 90%. Therefore, performance of the proposed interruption detection system is comparatively better considering the state-of-the-art system.

For the dynamic case. In the dynamic case, this study considers higher mobility of network nodes for generating dynamism in the system. It is accepted that the interloper is moving at a pace of 15m/s. The study changes the foundation used to focus the hubs that make up the IDS. It utilises the same basis utilised in connection with the static case. The main contrast is that now the interloper is thought to be portable. The results of this comparative study is demonstrated following.

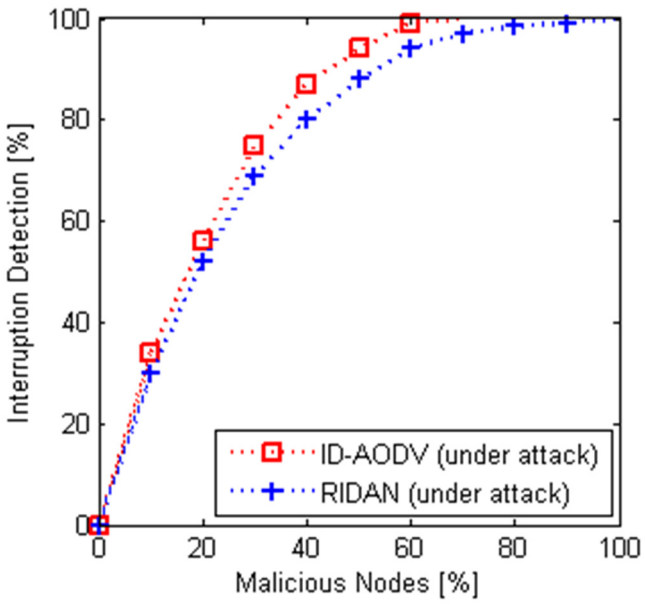

Fig 5. Comparative analysis of impact of percentage of malicious nodes on interruption detection under static condition.

doi:10.1371/journal.pone.0156885.g005

In Fig 6, a comparative analysis of impact of percentage of malicious nodes on interruption detection between the proposed ID-AODV and RIDAN systems is presented for the dynamic case. The results clearly states that the interruption detection rate of the proposed system is higher as compared the state-of-the-art system. This is because of the better mobility prediction and management while interruption detection using FSM based approach in the proposed system. Specifically, with 70% malicious nodes the proposed ID-AODV system is able to detect

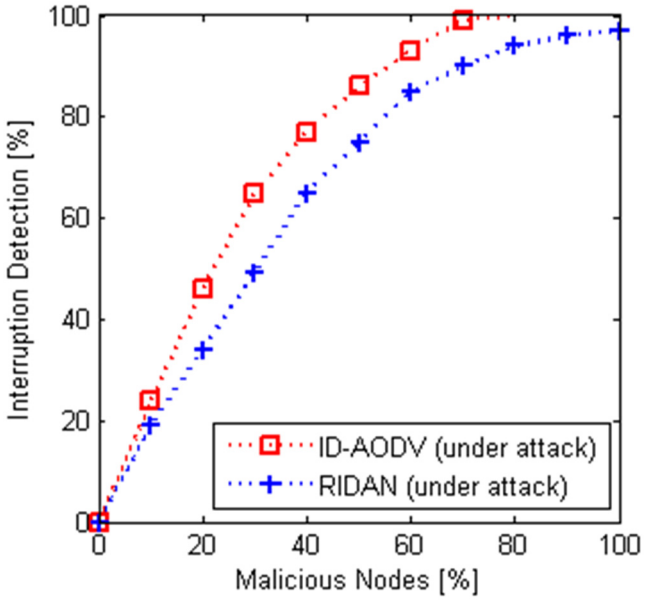

Fig 6. Comparative analysis of impact of percentage of malicious nodes on interruption detection under dynamic condition.

doi:10.1371/journal.pone.0156885.g006

Table 2. Comparison between RIDAN and ID-AODV in regards to Percentage of Detection.

% of malicious nodes	10	20	30	40	50	60	70	80	90	100
Static case										
ID-AODV	34	56	75	87	94	99	100	100	100	100
RIDAN	30	52	69	80	88	94	97	98.5	99	100
Dymanic case										
ID-AODV	24	46	65	77	86	93	99	100	100	100
RIDAN	19	34	49	65	75	85	90	94	96	98

doi:10.1371/journal.pone.0156885.t002

99% of malicious nodes where RIDAN systems is able to detect 88% of malicious nodes. RIDAN system is able to detect 98% of malicious nodes only when the percentage of malicious nodes reaches to almost 100%. Thus, performance of the proposed interruption detection system is comparatively better in comparison with the state-of-the-art system in dynamic case also. However, interruption detection percentage is lower in dynamic case as compared to the static case for the same percentage of malicious nodes for both the considered systems. Table 2 shows a clear comparison between ID-AODV and RIDAN in terms of average value and standard deviation.

Discussion

Response to Intrusions

This study's interruption location convention took into account either a dynamic or aloof reaction to interruptions. In regards to either reaction mode, the conclusion involved the disconnection of the culpable hub from the system. In the uninvolved mode, a hub settled on a one-sided choice focused on its own particular perceptions of irregular conduct. The more regular and anomalous the conduct from the pernicious hub, the sooner the meddlesome hub will be disengaged and be denied connection to the underlying system framework. The dynamic reaction mode offers a larger amount of certification than the latent mode. The expanded affirmation level is a result of a dominant part voting plan, and therefore the flooding of the meddling hub's personality through the system. The dynamic mode, then again, is more difficult to actualise.

In the case of Passive Response, once the edge esteem mitigating the impacts of connection mistakes for message misrouting or message alteration has been surpassed, an alert is raised. In the inactive mode, the hub that raised the caution expels the nosy hub from its neighbour table, and it takes part in further course revelations, Hello Messages or collective directing with the meddling hub. Furthermore the nosy hub's location is recorded in the Bad Node Table. This study presents in a later segment that as elements of analysis become subtler and the system becomes denser, there is a greater quantity of hubs that announce a hub meddling, and keep the pernicious hub from using the system assets. On the off chance that the hub being referred to keeps acting rudely, every hub in the system will inevitably settle on a one-sided choice to disassociate itself from the interloper. Dynamic Response proposes the Cluster Based Routing Protocol (CBRP), through which hub groups are structured, each with a chosen bunch head. The role of the bunch head involves upgrading the course revelation process.

Improvements. Reproductions utilising NS-2 have demonstrated that the AODV forms utilising the connection layer help in general to better bring about practically within all recreations. As previously mentioned, AODV has the preference that it adapts more data for each one appeal than it conveys. On the off chance that an appeal goes from S to D, and the answer from D to S, S will take into the course all moderate courses in the middle of S and D. This

implies that it is not important to convey the same number of solicitations for AODV. The source steering methodology is therefore useful in course revelation and course support cases. Otherwise, source directing is not appropriate for use in information bundles. Above all else, this includes a great deal of overhead. Besides it is not as conventional with respect to the example separation vector, or the connection express generally utilised as parts of the wired systems. This study's proposal based on these lines intends to execute a convention involving a blend of source directing and separation vector. Source directing ought to be utilised within the course revelation and course upkeep stages. These stages would likewise recognise that the directing tables are situated up progressively amid the spread of solicitations and answers. At the point when information parcels are sent, a separation vector calculation ought to be utilised. The bundles are basically sent to the next hop, as indicated by the directing table. This combined with the convention that stores a few courses for every goal, would likely mean a convention with an execution significantly better than the conventions reproduced in this postulation.

There are relatively few interruption discovery strategies proposed for Ad Hoc systems, and the field has not been totally investigated. This research accepts that the proposed IDS will have a positive effect on the interruption location for remote portable Ad Hoc systems. This study's interruption identification and reaction convention for MANETs have been shown to perform better than indicated by Stamouli et al. [6], in regards to false positives and rates of parcels conveyed. The connection changes and course changes are, with a high likelihood, straight capacities of the greatest rate and the hub stop time. In less upsetting situations ID-AODV beats all measurements with the exception of convention overheads. Interest conventions spread the connection changes faster, and diminish the parcel drop brought about by them. System clogging is the overwhelming explanation behind bundle drop. The convention's execution could be further enhanced if blockage is evaded.

Focal points of the proposed scheme

- The proposed plan causes no additional overhead, as it makes insignificant alterations to current information structures and capacities identified with posting a terrible hub in the current rendition of the unadulterated AODV.
- The proposed plan is more productive in regards to the created resultant courses, asset reservations and computational multifaceted natures.
- On the off chance that different noxious hubs work together, they will be thusly confined and segregated by their neighbours, on the grounds that they screen and act control over sending RREQs to hubs. Subsequently the plan effectively averts appropriated assaults.

Conclusion and Future Work

In this paper, a framework based on Finite State Machine (FSM) is presented for denial of service and intrusion detection in MANETs. Specifically, an Interruption Detection system for Adhoc On-demand Distance Vector (ID-AODV) protocol is presented based on finite state machine. From the design, implementation and evaluation of the proposed framework, following conclusions have been made. FSM based security measurement the proposed framework effectively recognizes packet dropping attack and sequence number attack. Under both types of attacks, packet delivery ratio of ID-AODV is higher as compared to the state-of-the-art techniques considering increasing number of CBR connections and speed of network nodes. For ID-AODV, Number of falsely marked hubs is lesser and malicious node detection rate is higher

considering increasing number of malicious nodes in the network. The overall interruption detection rate of ID-AODV is higher than that of RIDAN under both static and dynamic network conditions. Thus, State of the network nodes has decisive role in dynamic network environment such as MANETs. The framework can be utilized in developing sensitive and credible applications for MANETs. In future research, authors will evaluate the performance of ID-AODV under other types of security attacks. Prototype application development for MANETs using ID-AODV will also be a quest.

Supporting Information

S1 File. DoS and Intrusion Detection for MANET -2.
(PDF)

Author Contributions

Conceived and designed the experiments: MNA. Performed the experiments: OK. Analyzed the data: MNA. Wrote the paper: MNA. Built initial constructs and validated them in vitro and in vivo: MNA. Supervised the project and performed critical revision: OK. Improved the paper so that it is suitable for publication and wrote the Supplementary Information: AHA. Discussed the results and implications and commented on the manuscript at all stages: MNA AHA OK.

References

1. Visumathi J, Shunmuganathan KL. An Effective IDS for MANET Using Forward Feature Selection and Classification Algorithms. Procedia Engineering. 2012; 38:2816–2823.
2. Mamatha GS, Sharma SC. A robust approach to detect and prevent network layer attacks in MANETS. International Journal of Computer Science and Security. 2010; 4:275–284.
3. Wu B, Chen J, Wu J, Cardei M. A survey of attacks and countermeasures in mobile ad hoc networks. In Wireless Network Security. Springer US. 2007; 1:103–135.
4. Rafsanjani MK, Khavasi AA, Movaghar A. An efficient method for identifying IDS agent nodes by discovering compromised nodes in MANET. In Proceedings of the International Conference on Computer and Electrical Engineering. IEEE. 2009; 1:625–629.
5. Panaousis EA, Politis C, Birkos K, Papageorgiou C, Dagiuklas T. Security model for emergency real-time communications in autonomous networks. Information Systems Frontiers. 2012; 14:541–553.
6. Stamouli I, Argyroudis PG, Tewari H. Real-time intrusion detection for ad hoc networks. In Proceedings of the International Symposium on World of Wireless Mobile and Multimedia Networks, IEEE. 2005; 1: 374–380.
7. Perkins C, Belding-Royer E, Das S. Ad hoc On-Demand Distance Vector (AODV) Routing. Report, IETF. RFC 3561. 2003. Available: http://www.rfc-editor.org/info/rfc3561.
8. Jain AK, Tokekar V. Classification of denial of service attacks in mobile ad hoc networks. In Proceedings of the International Conference on Computational Intelligence and Communication Networks, IEEE.201; 1: 256–261.
9. Mutlu S, Yilmaz G. A distributed cooperative trust based intrusion detection framework for MANETs. In Proceedings of the International Conference on Networking and Services, 2011, 1: 292–298.
10. Xenakis C, Panos C, Stavrakakis I.A comparative evaluation of intrusion detection architectures for mobile ad hoc networks. Computers & Security, 2011; 30:63–80.
11. Nadeem A, Howarth MP. A survey of MANET intrusion detection & prevention approaches for network layer attacks. Communications Surveys & Tutorials, IEEE, 2013; 15:2027–2045.
12. Kheyri D, Karami M. A comprehensive survey on anomaly-based intrusion detection in MANET. Computer and Information science. 2012; 5:132–144.
13. Nadeem A, Howarth M. Adaptive intrusion detection & prevention of denial of service attacks in MANETs. In Proceedings of the International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly, ACM. 2009; 1: 926–930.
14. Joseph JFC, Lee BS, Das A, Seet BC. Cross-layer detection of sinking behavior in wireless ad hoc networks using SVM and FDA. IEEE Transaction on Dependable and Secure Computing. 2011; 8:233–245.

15. Damopoulos D, Menesidou SA, Kambourakis G, Papadaki M, Clarke N, Stefanos G. Evaluation of anomaly-based IDS for mobile devices using machine learning classifiers. Security and Communication Networks. 2012; 5:3–14.
16. Li W. Using genetic algorithm for network intrusion detection. In Proceedings of the United States Department of Energy Cyber Security Group. 2004; 1:1–8.
17. Ahmed A, Lisitsa A, Dixon C.A misuse-based network intrusion detection system using temporal logic and stream processing. In Proceedings of the International Conference on Network and System Security, IEEE. 2011; 1:1–8.
18. Stakhanova N, Basu S, Wong J. On the symbiosis of specification-based and anomaly-based detection. Computers & Security. 2010; 29:253–268.
19. Ilgun K, Kemmerer RA, Porras PA. State transition analysis: A rule-based intrusion detection approach. IEEE Transactions on Software Engineering. 1995; 21:181–199.
20. Tseng CY, Balasubramanyam P, Ko C, Limprasittiporn R, Rowe J, Levitt K. A specification-based intrusion detection system for AODV. In Proceedings of the workshop on Security of ad hoc and sensor networks, ACM. 2003; 1: 125–134.
21. Tamilselvan L, Sankaranarayanan V. Solution to prevent rushing attack in wireless mobile ad hoc networks. In proceeding of the Symposium on Ad Hoc and Ubiquitous Computing, IEEE. 2006; 1:42–47.
22. Djahel S, Nait-Abdesselam F, Zhang Z. Mitigating packet dropping problem in mobile ad hoc networks: proposals and challenges. IEEE Communications Surveys & Tutorials. 2011; 13:658–672.