Performance Evaluation of DSR, ARIADNE, AODV and SAODV Protocols in Mobile Ad hoc Networks

Rupinder Kaur Gurm[1] Aarti Kaushal[2] Manshi Sukhla[3] Jasmeet Singh[4]
Assitant Professor CSE Department[1,3,4]
Assistant Professor MCA Department[2]
RIMT-IET, Mandigobingarh[1234]

Abstract. Mobile ad hoc networks will be an integral part of next generation networks because of its flexibility, infrastructure less nature, ease of maintenance, auto configuration, self administration capabilities, and cost effectiveness. This research paper shows comparative evaluation within mobile ad hoc networks' routing protocols from reactive, proactive and hybrid categories. We have comprehensively analyzed the results of simulation for mobile ad hoc routing protocols for quality of services of end to end delay, media access delay, throughput and packet delivery ratio for optimized link state routing, temporary ordered routing algorithm and ad hoc on demand distance vector protocol. In mobile ad hoc networks, mobile nodes must collaborate with each other in order to interconnect, organize the dynamic topology as mobility cause route change and establish communication over wireless links. A performance evaluation of routing protocol is very cumbersome due to various metrics involving dynamic topologies, mobility, routing limited resources, security etc. One common method to conduct research in the networking and security fields is to simulate and evaluate the protocol(s) in various scenarios. Fortunately, there are various computer simulation applications that are available for doing those tasks, such as NS-2 [22], OPNET [23], GLOMOSIM [24], etc. My thesis is heavily based on the implementation and experiments in the OPNET simulation environment. OPNET Modeler [23] was chosen as a simulation environment because it is one of the leading environments for network modeling and simulation. It supports large number of built-in industry standard network protocols, devices, and applications. In addition, its programming library helps researchers to easily modify the network elements and measure their performance in the simulation environment. OPNET also provides rich data analysis features.

Keywords: Adhoc Network, Routing, Classification, Attacks, Secure Routing Protocols, MANET, QoS, Routing Protocol, Wireless1. Introduction

I. INTRODUTION

Mobile Ad-hoc network is a set of wireless devices called wireless nodes, which dynamically connect and transfer information. Wireless nodes can be personal computers (desktops/laptops) with wireless LAN cards, Personal Digital Assistants (PDA), or other types of wireless or mobile communication devices. Figure 1.1 illustrates what MANET Is? In general, a wireless node can be any computing equipment that employs the air as the transmission medium. As shown, the wireless node may be physically attached to a person, a vehicle, or an airplane, to enable wireless communication among them. In MANET, a wireless node can be the source, the destination, or an intermediate node of data transmission. When a wireless node plays the role of intermediate node, it serves as a router that can receive and forward data packets to its neighbor closer to the destination node. Due to the nature of an ad-hoc network, wireless nodes tend to keep moving rather than stay still. Therefore the network topology changes from time to time.

Figure1.1: Types of Wireless or Mobile Communication Devices

Wireless ad-hoc network have many advantages:

- *Low cost of deployment*: Ad hoc networks can be deployed on the fly; hence no expensive infrastructure such as copper wires or data cables is required.
- *Fast deployment*: Ad hoc networks are very convenient and easy to deploy since there are no cables involved. Deployment time is shortened.
- *Dynamic Configuration:* Ad hoc network configuration can change dynamically over time. When compared to configurability of LANs, it is very easy to change the network topology of a wireless network.

MANET has various potential applications. Some typical examples include emergency search-rescue operations, meeting events, conferences, and battlefield communication between moving vehicles and/or soldiers. With the abilities to meet the new demand of mobile computation, the MANET has a very bright future.

II. CURRENT CHALLENGES

In a mobile ad hoc network, all the nodes cooperate with each other to forward the packets in the network, and hence each node is effectively a router. Thus one of the most important issues is routing. This thesis focuses mainly on routing issues

in ad hoc networks. In this section, some of the other issues in ad hoc networks are described:

- *Distributed network:* A MANET is a distributed wireless network without any fixed infrastructure. That means no centralized server is required to maintain the state of the clients.
- *Dynamic topology:* The nodes are mobile and hence the network is self-organizing. Because of this, the topology of the network keeps changing over time. Consequently, the routing protocols designed for such networks must also be adaptive to the topology changes.
- *Power awareness:* Since the nodes in an ad hoc network typically run on batteries and are deployed in hostile terrains, they have stringent power requirements. This implies that the underlying protocols must be designed to conserve battery life.
- *Addressing scheme:* The network topology keeps changing dynamically and hence the addressing scheme used is quite significant. A dynamic network topology requires a ubiquitous addressing scheme, which avoids any duplicate addresses. In wireless WAN environments, Mobile IP [10] is being used. Because the static home agents and foreign agents are needed, hence, this solution is not suitable for ad hoc network.
- *Network size:* The ability to enable commercial applications such as voice transmission in conference halls, meetings, etc., is an attractive feature of ad hoc networks. However, the delay involved in the underlying protocols places a strict upper bound on the size of the network[30].
- *Security:* Security in an ad hoc network is extremely important in scenarios such as a battlefield. The five goals of security – availability, confidentiality, integrity authenticity and non-repudiation - are difficult to achieve in MANET, mainly because every node in the network participates equally in routing packets.

III. THESIS TARGET

The mobile ad hoc network is a new model of wireless communication and has gained increasing attention from industry. As in a general networking environment, mobile ad-hoc networks have to deal with various security threats. Due to its nature of dynamic network topology, routing in mobile ad-hoc network plays a vital role for the performance of the networks. It is understandable that most security threats target routing protocols – the weakest point of the mobile ad-hoc network. There are various studies and many researches in this field in an attempt to propose more secure protocols [1][2][16].

However, there is not a complete routing protocol that can secure the operation of an entire network in every situation. Typically a "secure" protocol is only good at protecting the network against one specific type of attacks. Many researchers have been done to evaluate the performance of secure routing protocols in comparison with normal routing protocols [1][4][6]. One of the objectives of this research is to examine the additional cost of adding a security feature into non-secure routing protocols in various scenarios. The additional cost includes delay in packet transmission, the low rate of data packets over the total packets sent, etc.

It is well known that the real-world network does not operate in an ideal working environment, meaning that there are always threats and malicious actions affecting the performance of the network. Thus, studying the performance of secure routing protocols in malicious environments is needed in order to effectively evaluate the performance of those routing protocols. In the thesis, I have implemented two secure routing protocols: a secure version of the dynamic source routing - DSR (ARIADNE) [1] and Secure Ad hoc On-demand Distance Vector routing protocol (SAODV)[2] in the OPNET simulation environments [23]. I will also create malicious scenarios by implementing several attacks in the simulation environments.

By implementing secure routing protocols and running these two routing protocols in malicious environments, I have evaluated those secure routing protocols, and have proposed solutions to remove the weaknesses and/or to improve the performance of these secure routing protocols.

IV. ROUTING PROTOCOLS EXPERIMENTAL RESULTS

In this phase, the performance data of four routing protocols (DSR, ARIADNE, AODV and SAODV) are collected. A scenario is set up for data collection. This scenario is run 11 times with 11 different values of the mobility *pause time* ranging from 0 to 100 seconds. The data is collected according to two metrics – *Packet Delivery Fraction* and *Normalized Routing Load*. In general, the actual values of the performance metrics in a given scenario are affected by many factors, such as node speed, moving direction of the nodes, the destination of the traffic, data flow, congestion at a specific node, etc. It is therefore difficult to evaluate the performance of a protocol by directly comparing the acquired metrics from individual scenarios. In order to obtain representative values for the performance metrics, we decided to take the average values of multiple simulation runs. The average values of these 11 simulation runs are then calculated for the two metrics and used as a baseline to evaluate the performance of routing protocols in malicious environments.

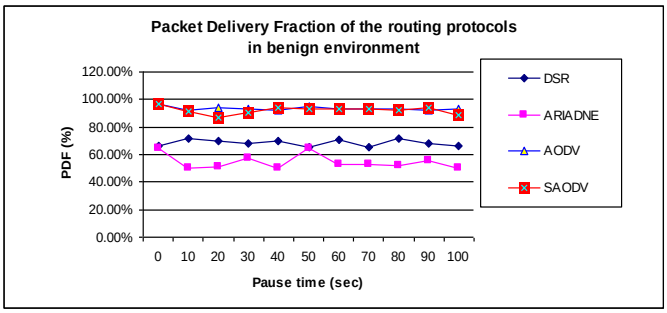

Figure 1.2: Packet Delivery Fraction vs. pause time values in benign environment

As shown in Figure 1.2, the percentage of packets delivered in AODV and SAODV is fairly close to each other, and both

methods exhibit superior performance (~90% in general). The security features in SAODV lower the performance a little bit. Actually, the generation and verification of digital signatures depends on the power of the mobile nodes and causes a delay in routing packet processing[28]. In the simulation environments, this delay depends on the simulation running machine and is not high enough to make the significant difference for the PDF metric. On the other hand, the packet delivery fraction in DSR and ARIADNE are 20-40% lower than that of AODV/SAODV across the board given different mobility pause times.

The major difference between AODV and DSR is caused by difference in their respective routing algorithms. It was reported by other researchers [5] [7] that, in high mobility and/or stressful data transmission scenarios, AODV outperforms DSR. The reason is that DSR heavily depends on the cached routes and lack any mechanism to expire stale routes. In the benign environment of our experiments, the default expiry timer of cached route for DSR and ARIADNE is 300 seconds, while this number is 3 seconds for AODV and SAODV. In respect to the protocol design, these values are kept unchanged through all the simulation scenarios. Furthermore, DSR and ARIADNE store the complete path to the destination. Hence, if any node moves out of the communication range, the whole route becomes invalid. In MANETs, the nodes are mobile, so route change frequently occurs. Without being aware of most recent route changes, DSR may continue to send data packets along stale routes, leading to the increasing number of data packets being dropped.

The situation is even worse for ARIADNE, mainly because ARIADNE relies on the delayed key disclosure mechanism of TESLA when authenticating packets, including the RERR packets. When an intermediate node in ARIADNE notices a broken link, it sends a RERR message to the source node of the data packet. The source node, however, simply saves the RERR message, because it has not yet received from the intermediate node the key needed to authenticate the route error. The source node keeps sending the data until the second route error is triggered, and another RERR is received. Only then would the previous route error be authenticated, and the broken link not be used any more. This explains the worse performance of ARIADNE in comparison with DSR and other protocols [19].

As shown in Figure 1.3, the NRL metric is, in general, inversely proportional to the PDF metric (Figure 1.2). A low PDF value (for example, ARIADNE in Figure 1.2) corresponds to a high NRL value (Figure 1.3). This relationship between PDF and NRL is further illustrated in Table 1.1, which lists the average values of the two metrics over 11 simulation runs for each of the four protocols. The comparison between the normal routing protocols (DSR and AODV) and their respective secure version (that is, ARIADNE and SAODV) in benign environments has been extensively conducted by other researchers [1][4][6]. In the next section, I will discuss the performance of the protocols in various malicious environments.

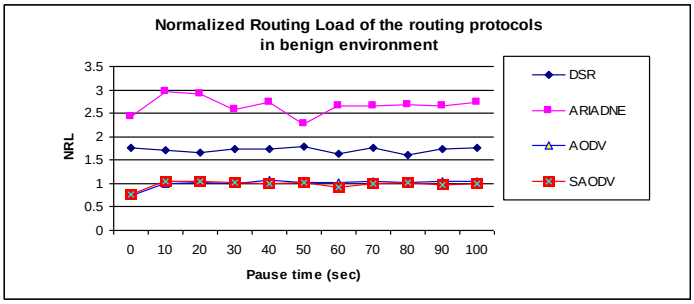

Figure 1.3: Normalized Routing Load vs. pause time values in benign environment

Pause Time (seconds)	Packet Delivery Fraction (%)	Normalized Routing Load
DSR	68.41%	1.72
ARIADNE	54.70%	2.58
AODV	93.45%	1.01
SAODV	92.00%	0.98

Table 1.1: The "*baseline*" metrics of the four protocols

I.

1. Route Drop attack

The Route Drop [14] attacks affect all kinds of routing protocols. The Route Drop attack may trigger more routing packets within the network. Once a route request packet is sent, the source node expects to receive the route reply within a period of time. If no route reply is received, it will keep sending the route request packet until the data in the source node's sending queue times out and is dropped. Figure 5.3 shows the effect of such an attack on the packet delivery fraction (PDF) metric, given different number of malicious nodes. Figure 1.4(A) shows the performance of DSR and ARIADNE; and Figure 1.4(B) shows the performance of AODV and SAODV. It is noticeable that, when the number of malicious nodes increases, the percentage of data packets received by the destination node decreases.

In a MANET, the RREQ packets are sent in a broadcast mode. If a node selfishly refuses to send routing packets and discards it, the routing packets can still be received and forwarded by other nodes. Consequently, the data packet still finds its way to the destination. Therefore, a single malicious node may not affect the number of received data packets. On the other hand, if the malicious node is in a position that it is the only way to the destination or if the malicious node is the destination node itself, it will not reply to the RREQ. It is obvious that in such a situation the data packet will not get to the destination and will be dropped. Consequently, the number of received data packets will decrease.

Also shown in Figure 1.3 is that there are some special cases where the PDF metric actually increases when the number of malicious node increases. For example, in DSR's PDF metric

graph, when the number of malicious nodes changes from 3 to 4 nodes, the DPF metric goes up by 5%. Our preliminary analysis has led us to believe that such anomaly might be caused by the positions of the malicious nodes, the motion of the mobile nodes, and the number of broken links. For AODV and SAODV, the impact of increasing number of malicious nodes on the PDF metric is less than that in the case of DSR and ARIADNE. When the number of malicious nodes is one or higher, the PDF values appear to remain almost constant. The cause of this phenomenon is tied to the nature of AODV and SAODV protocols. They use a standard IP routing table, and use only one route for a destination. A route expires if it is not recently used after a pre-determined elapsed time (the default value is 3 seconds in the OPNET simulator [25]). When the nodes move, some routes may break. AODV and SAODV trigger a new discovery process to find new routes. This feature helps to ease the effect of Route Drop attack in AODV and SAODV. It, however, is not the case for DSR and ARIADNE, in both of which the PDF metric goes down when the number of malicious nodes goes up. If the mobility of the nodes is high, the PDF metric also goes down [7]. The combined impact makes DSR and ARIADNE more vulnerable to this type of attacks.

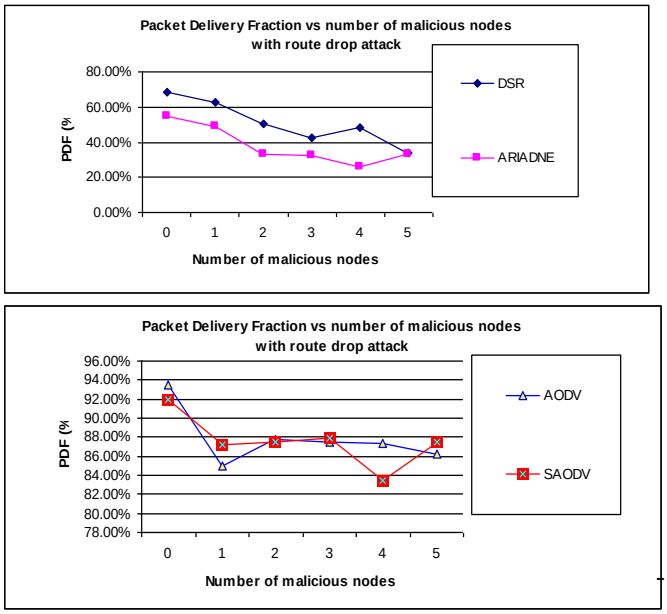

Figure 1.4: Packet Delivery Fraction vs. number of malicious nodes with route drop Attack

Figure 1.5(A) and (B) represent the NRL metric of the protocols. The NRL metric evaluates the efficiency of the routing protocol. It depends on both the number of data packets received and the number of routing packets sent. It can be inferred that, when the number of malicious nodes is equal to the number of nodes in the network, the PDF metric will be down to 0 and the number of routing packets sent will be equal to the number of RREQ packets, and the NRL metric will go to infinity. As shown in Figure 1.5, when the range of malicious nodes is from 1 to 5, the NRL metric of DSR and ARIADNE, and that of AODV and SAODV go in different directions. The NRL metric of DSR and ARIADNE increases (when the number of malicious nodes increases), while the NRL metric of AODV and SAODV go level.

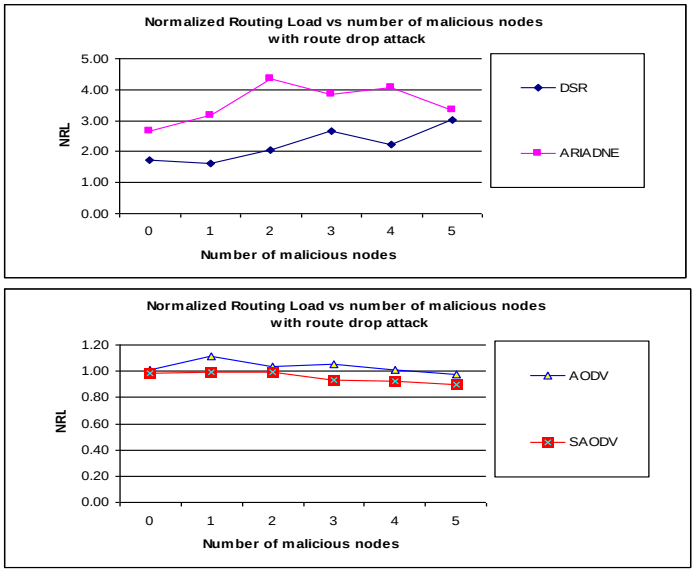

Figure 1.5: Normalized Routing Load vs. number of malicious nodes with route drop attack

Such differences between the two sets of protocols are related to the settings of those protocols. By default, for DSR and ARIADNE, the maximum request retransmission number is 16, while the number of route request retries in AODV and SAODV is only 5 [25]. That means that, for a route discovery to a destination, DSR and ARIADNE will try more times than AODV and SAODV, if no route reply is received. In the case of route drop attacks, most of the routing packets dropped are RREQ, so the data source node keeps sending the RREQ until the number of RREQ retries reaches the maximum number. When the number of malicious node increases, the difference in routing packet sent is bigger. Furthermore, the number of received data packets is down with respect to the number of malicious nodes. All of these explain the differences in NRL metric among the protocols.

Conclusion

In general, when the number of malicious nodes increases, the number of received data packets or PDF metrics decreases.
The PDF metric of ARIADNE and DSR is more negatively affected by this type of attacks than AODV and SAODV, when the number of malicious nodes increases and when the mobility of the nodes is high.
The impacts of the attacks on DSR and ARIADNE are similar, because the route discovery mechanisms of the two protocols are the same and the route maintenance mechanisms of the two protocols are also the same[20].
The initial position, movement of the malicious nodes affects the number of received data packets. That means, when the initial position of a malicious node changes, it may cause the number of received data packets to go up. Further study is

needed to evaluate the impact of the mobility of the malicious nodes on the operation of the protocols.

- A mechanism is needed to detect malicious nodes with the route drop attacks, in order to isolate these nodes from the routing process.

2. Route modification

This type of attacks changes the content of RREP routing packets [19] [26]. The secure routing protocols (ARIADNE and SAODV) are designed to detect these changes and discard the changed RREP routing packets. Of course, when the changed routing packets are dropped, more will be generated in order to find the routes. It is our hypothesis that, without protection against route modification, normal protocols (DSR and AODV) will be negatively affected by this type of attacks. In this section, the impacts of the attacks on the protocols are studied.

It is noticeable in Figure 1.6 that, for DSR and AODV, when the number of malicious nodes increases, the number of data packets dropped by them also increases. This accounts for the decline in the PDF metric of DSR and AODV, the two "insecure" protocols. As expected, the PDF metric of ARIADNE and SAODV nearly remains unchanged.

It is interesting to note that the fifth malicious node helps to increase the ARIADNE's PDF metric. This "anomaly" is similar to the special case of DSR in Figure 5.3 when the number of malicious nodes in four. In this scenario, the phenomenon is caused by the position of the fifth malicious node[32]. I tried re-assigning the role of the fifth malicious node to node number 0, and the number of received data packets decreased. Again our preliminary conclusion is that the position of the malicious nodes affects the number of received data packets and the PDF metric. For the DSR protocol, it is obvious that the protocol is heavily affected by the route modification attack, especially when the number of malicious nodes is 3 or higher. The malicious node modifies the source route in the RREP packets to make it itself more attractive to the data source nodes. Due to the promiscuous listening features of DSR [8][12], the nodes that can listen to the RREP also may update their route cache with wrong routes. This feature of DSR causes the attack even more severe by spreading out the wrong routes. The way the route modification attack is launched in AODV is different from that in DSR. In AODV, the malicious node just increments the route sequence by 1 and decrements the hop count by 1. This attack is less successful than the route modification attack in DSR. For AODV, the nodes do not keep the complete route, but the address of the neighbor that sends the routing packet. In particular, route listening is limited to the source of any routing packets being forwarded [7][9][14]. This usually causes AODV to rely on a route discovery mechanism more often. This feature helps AODV eases the impacts of the attacks. The NRL metrics of the protocols are shown in Figure 1.7. For ARIADNE protocol, the NRL metric is stable. It is inversely proportional to the number of received data packets.

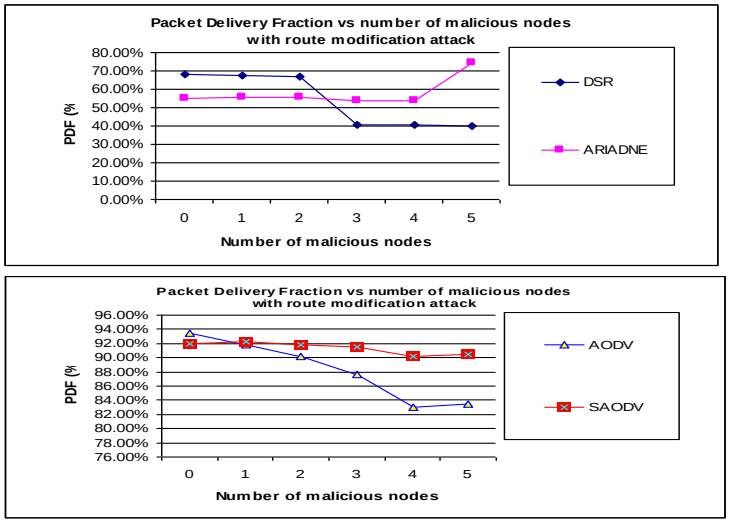

Figure 1.6: Packet Delivery Fraction vs. number of malicious nodes with Route modification attack

Due to the attack, some RREP packets are changed and detected by ARIADNE. In order to find a route, the source node in ARIADNE keeps sending the RREQ, but the number of new RREQ packets is too small to have a negative impact on the NRL metric of ARIADNE. For DSR, when the number of malicious node increases, the number of received data packets decreases as well, and the NRL metric goes up accordingly. The AODV protocol is also fooled by the attack. There are no new routing packets generated, so the number of routing packets is nearly constant.

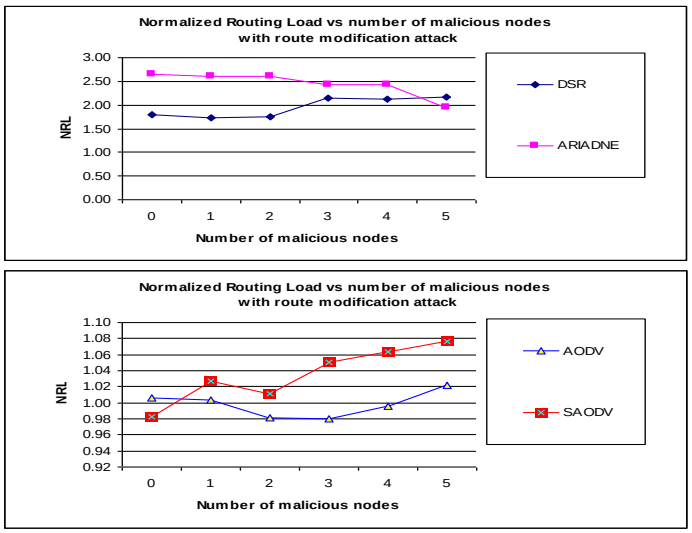

Figure 1.7: Normalized Routing Load vs. number of malicious nodes with route modification attack

Consequently, the NRL metric is inversely proportional to the number of received data packets. That means the NRL metric slightly goes up when the number of malicious nodes increases. The situation is different with SAODV, due to its detecting and discarding changed routing packets. Many more

routing packets are sent [5][6] to find a new route. This reason causes the NRL metric of SAODV to go up. The slight delay and congestion in the network due to many more routing packets also accounts for the increase of NRL metric.

Conclusion:

- This type of attack negatively affects the DSR and AODV protocols. When the number of malicious nodes increases, the protocols failed to deliver the data to the destinations. It is shown by the experimental results that the PDF metric goes down and the NRL metric goes up.
- DSR is affected more by this type of attacks than AODV is. It is shown by the experimental results that the difference in the PDF metric of DSR, between the cases when there is no attack and when there is an attack, is bigger than that of AODV.
- This type of attack does not fool the secure protocols, but it has a negative effect in the networks by triggering more routing packets to be sent. To some extent, it can congest the networks with routing packets and cause the data packets to be dropped due to no route being found.
- The impact on DSR is heavier than AODV, when the number of malicious nodes increases, mainly due to the different nature of the attacks and the different operations of the protocols.

The initial position, movement of malicious nodes also affects the PDF metric. That means, when the initial position of a malicious node changes, it may cause the number of received data packets to go up.

-

3. Route fabrication

This attack applies to the DSR and the ARIADNE protocols. The route fabrication [19][26] attack will succeed with both DSR and ARIADNE when the *cached route reply* feature is enabled. When the number of malicious nodes increases, the number of received data packets decreases, and the NRL increases. Hereunder, the experimental result is studied.

As shown in Figure 1.8, the PDF metric decreases when the number of malicious nodes increases. As in the case of route modification attack, there is a special case when the fifth malicious node is added, in which the PDF metric goes up again. Our explanation to this anomaly is as follows. The initial position of the fifth malicious node is close to the edge of the network. When it receives a RREQ, it will return a RREP to the source node, to tell that it is only one hop away to the destination. That is true though it has no such route in its cache. It unintentionally speeds up the route discovery phase. During the simulation time, the destination nodes move closer to the source than the malicious node and the data packets still get to the destinations. Because the packets get to destination nodes before traversing the whole source route, the route is shortened then a gratuitous route reply is sent [12]. Due to the promiscuous listening feature [8][12] of DSR and ARIADNE, the other nodes also update their route caches like in the case of route modification. When a node needs to send a data packet, it uses its cached route. During the simulation time, the intermediate nodes use their cached routes to forward successfully the data packet to the destination.

I tried changing the initial position of the fifth malicious node further toward the middle of the network, and had observed the drop of the PDF metric.

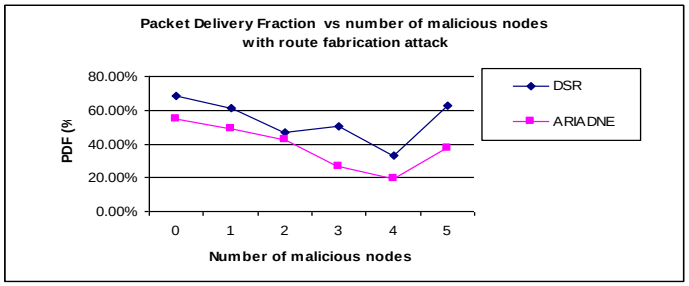

Figure 1.8: Packet Delivery Fraction vs. number of malicious nodes for DSR/ARIADNE with fabrication attack

When the number of the malicious nodes increases, the number of data packets received by the destination decreases. As shown in Figure 1.9, that leads to increased NRL (when the number of routing packets remains almost the same).

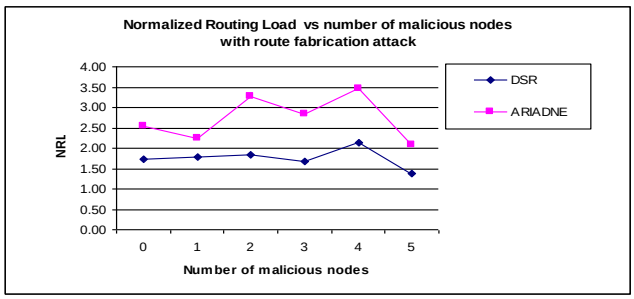

Figure 1.9: Normalized Routing Load vs. number of malicious nodes for DSR/ARIADNE with fabrication attack

Conclusion

DSR and ARIADNE are obviously affected by the route fabrication attack, if the *cached route reply* feature is enabled. When the number of malicious nodes increases, the PDF metric decreases and the NRL metric increases. ARIADNE needs to be improved in this regard to secure the route reply from intermediate nodes.

The initial position and movement of the malicious nodes can affect the number of received data packets. That means, when the initial position of a malicious node changes, it may cause the number of received data packets to go up (even when the total number of malicious nodes have increased).

4. Impersonation

This attack applies to the AODV and the SAODV protocols. It is known that SAODV relies on the digital signature authentication scheme.However, if the digital signature is used without public key verification or a key management center, the malicious nodes may still successfully launch the attack. In

this session, the performance of AODV and SAODV with and with out public key verification is studied[21].

As shown in Figure 1.10, SAODV and AODV are both vulnerable when the public key verification is not in effect. The impact of malicious nodes on the PDF metric is obvious. When the number of malicious nodes increases, the PDF metric of AODV and SAODV (without public key verification) decreases. The PDF metric of SAODV with public key verification remains almost the same.

It should be noted that SAODV with public key verification may have its own unique overhead. As mentioned by the author of SAODV [2], a key management sub-system is assumed to be available in the network. However, in a MANET, every node tends to have the same role. If the role of key management is assigned to a certain node, that node may become a single point of failure, and therefore a vulnerability of the network.

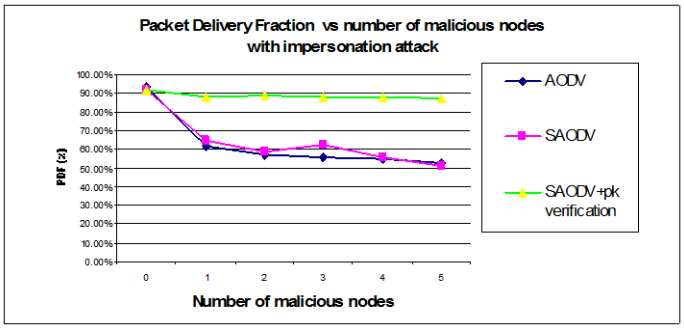

Figure 1.10: Packet Delivery Fraction vs. number of malicious nodes for AODV/SAODV with impersonation attack

When the number of data packets received goes down (caused by the increased number of malicious nodes), the number of routing packets change slightly, resulting in the higher NRL metrics (as shown in Figure 1.11). The only exception is in the case of SAODV with public key verification, in which the NRL metrics remain almost the same, even given increased number of malicious nodes.

Conclusion

AODV and SAODV without pubic key verification are vulnerable to impersonation attacks. The impacts on the two protocols are similar. The more the number of malicious nodes in the network is, the fewer the number of received data packets is.

- As shown by the experiments, SAODV is secure against impersonation attack only when there is a way to verify the public key of the route reply originator. In other words, a key management center is really necessary to make SAODV secure against impersonation attacks. This is still an outstanding issue of SAODV [2].

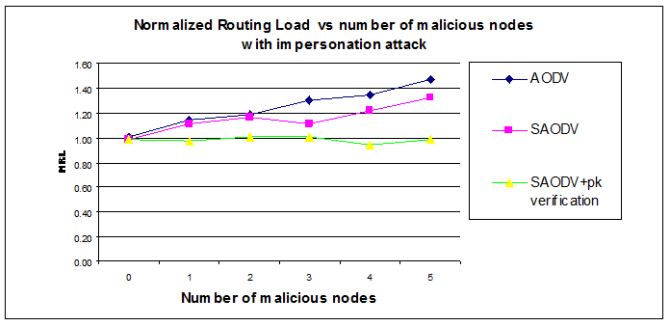

Figure 1.11: Normalized Routing Load vs. number of malicious nodes for AODV/SAODV with impersonation attack

V CONCLUSION

In this paper, the four routing protocols (DSR, OADV, ARIADNE and SAODV) are evaluated first in a benign environment and then in various malicious environments. Hereunder is the conclusion of the evaluations:

- In a benign environment, given the network setup and mobility model, AODV and SAODV outperform DSR and ARIADNE. The difference is due to the high mobility of the nodes, and as such the negative impact upon the operations of the DSR and ARIADNE protocols in such environment.
- The route drop attacks cause the number of received data packets to decrease for all of the protocols. When the number of malicious nodes increases, fewer data packets can get to the destination.
- The secure protocols (ARIADNE and SAODV), working in malicious environments with route modification attacks, have achieved almost the same high PDF metric as in the benign environments. There is a slight decrease of PDF metric due to more routing packets being generated. In general, the NRL metric is higher when the number of malicious nodes increases.
- On the other hand, in all simulated malicious environments, the normal routing protocols (DSR and AODV) have failed to get data delivered to the destinations. In general, when the number of malicious nodes increases, the PDF metric decreases. The level of impact by the attacks is different among the protocols, but DSR appears to be more vulnerable to the attacks than AODV, mainly due to the different underlying operations of the protocols.
- It is noticed that the initial position of the nodes may affect the number of received data packets. As observed in the experiments, positioning the malicious nodes initially in the middle of the network affects the PDF metrics the most.
- The ARIADNE protocol does not properly handle the case in which the intermediate nodes return cached routes. If the feature is enabled in order to take advantage of faster route discovery time, the protocol may become vulnerable to fabrication attacks. This vulnerability must be removed in order for the *cached route* feature to be effectively used.

- The SAODV protocol really needs a key management mechanism to work properly in malicious environments. There are many researches related to this issue [28][29][30]. Certificate-based authentication is a possible solution to this issue, in which the authentication process is distributed amongst a set of nodes in the networks.

Intrusion detection is a problem of great significance to protecting information systems security, especially in view of the worldwide increasing incidents of cyber attacks. Since the ability of an IDS to classify a rage variety of intrusions in real time with accurate results is important, we will consider performance measures in three critical aspects: training and testing times; scalability; and classification accuracy. Since most of the intrusions can be located by examining patterns of user activities and audit records (Denning, 1987), many IDSs have been built by utilizing the recognized attack and misuse patterns. IDSs are classified, based on their functionality, as misuse detectors and anomaly detectors. Misuse detection systems use well-known attack patterns as the basis for detection.

This thesis focuses on the detection of attacks in Wireless networks (802.11b). As the Mobile Adhoc Networks has some inherent flaws, it is prone to different attacks. The widespread deployment of Mobile Adhoc Networks makes detection of attacks on these networks essential. This work uses an agent-based system called Cougaar Intrusion Detection System (CIDS) developed at the ISSRL lab for Mobile Adhoc Networks , which was earlier used for detection of attacks in wired networks. Presented in this work are some specific features of CIDS along with a modified monitor agent to detect attacks in Mobile Adhoc Networks . The CIDS is an efficient tool that uses intelligent techniques like Fuzzy Decision System to detect different attacks in the network. To test the efficiency of the system, three of the most common attacks that occur on a Mobile Adhoc Networks are implemented and these are detected using the modified CIDS. Two of these attacks are launched in a real environment and the remaining one is performed using a network simulator, NS2. Some of these attacks are launched in an ad-hoc network and the others are tested in an infrastructure network. Accordingly, data are collected; preprocessed and fuzzy rules are generated for different attack detection. The results indicate that in all the three cases CIDS was able to detect the attacks with good detection rate.

REFERENCES

1. FIPS-197. Advanced Encryption Standard Park, Vol. 3, no. 3, p. 237–246.
2. Netherlands, Baltzer ACM Press, 1998.
3. Kaufman Charlie, Perlman Radia, Speciner Mike. Network Security: Private Commu- nication in a Public Wold, 2nd ed., USA, Prentice Hall PTR, 2002.
4. Levington M. Unlocking the secret of wireless security. In Oen, p. 23 United Kingdom, Wilmington Business Publishing, Sept. 2002.
5. IEEE Std 802.11. Physical Layer (PHY) Institute of Electrical and Electronics Engineers, Inc. September 1999.
6. Arbaugh, W. A., Shankar, N. and Justin Wan, Y.C. Your 802.11 Wireless Network has No Clothes, [online], March 2001, referred 20.3.2003,
7. Borisov, N., Goldberg, I. and Wagner, David. Security of the WEP algorithm. [online], referred 20.3.2003,
8. Prasad, A.R, Moelard, H. , Kruys, J. Security Architecture for Wireless LANs: Cor- porate and Public Environment. In VTC2000–Spring Confrence proceedings, Part 1. , Vol. 1, p. 283–287. Piscataway, USA, IEEE, 2000.
9. Hill, Joshua. An Analysis of the RADIUS Authentication Protocol. [online], referred 20.3.2003, URL: http://www.untruth.org/ josh/security/radius/radius-auth.html.
10. Williams Joseph. Providing for Wireless LAN Security, Part 2. In IT Professional, Vol. 4, no. 6, p. 44–48. USA, IEEE, Nov.–Dec. 2002.
11. Rautpalo, Jussi. Implementing secure Wireless Local Area Network Access. Master's Thesis, Helsinki University of Technology, 2002.
12. Advanced Encryption Standard - Wikipedia. [online], referred 12.4.2003, URL: http://www.wikipedia.org/wiki/AES.
13. Ferguson, N., Kelsey, J., Lucks, S. et al. Improved Cryptanalysis of Rijndael. [on- line], referred 14.4.2003, URL: ttp://www.macfergus.com/pub/icrijndael.pdf.
14. Fluhrer, S., Mantin, I. and Shamir, A. Weaknesses in the Key Scheduling algorithm of RC4. [online], referred 14.2003, URL: http://citeceer.nj.nec.com/fluhrer01.html.
15. Wright, Joshua. Detecting Wireless LAN MAC Address Spoofing. [online], referred17.5.2003, URL: http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf. december 2.
16. Erten, Y.M. A layered security architecture for corporate 802.11 wireless networks., 14-15 May2004,123-128.
17. Feil, H. 802.11 Wireless Network Policy Recommendation For Usage Within Unclassified Government Networks. The Aerospace Corporation, 2003, 832-838.
18. Fluhrer, S., Shamir, A. and Mantin, I. Weaknesses in the Key Scheduling Algorithm of RC4. Selected Areas of Cryptography, Toronto, Canada, 2001.
19. Perkins, E. B. Royer, S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing - Internet Draft", RFC 3561, IETF Network Working Group, July 2003.
20. C. E. Perkins and E. M. Royer, "Ad-Hoc On Demand Distance Vector Routing", Proceedings of the 2nd IEEE Workshop New Orleans, LA, 1999, pp. 90-100.
21. C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance vector routing (DSDV) for mobile computers", Proceedings of ACM SIGCOMM 94, 1994, pp. 34–244.
22. D. Bertsekas and R. Gallager, "Data Networks" Prentice Hall Publ., New Jersey, 2002.
23. D. B. Johnson, D. A. Maltz, Y.C. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", IETF Draft, April 2003, work in progress. http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt
24. D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc Networks", Mobile Computing, Kulwer Publ., 1996, pp. 152-81.
25. V. Nazari, K. Ziarati, "Performance Comparison of Routing Protocols for Mobile Ad hoc Networks", IEEE 2006.
26. V. Park and S. Corson, Temporally Ordered Routing Algorithm (TORA) Version 1, /draft-ietf-manet-tora-spec-01.txt, 1998
27. H. Ehsan and Z. A. Uzmi (2004), "Performance Comparison of Ad HocWireless Network Routing Protocols", IEE,E 8th International Multitopic Conference, Proceedingsof INMIC, December 2004, pp.457 – 465.
28. Iskra Djonova Popova, "A PowerPoint presentation on Routing in Ad-hoc Networks", 9th CEENet Workshop on Network Technology, Budapest 2004.
29. J. Broch, D.A. Maltz, D. B. Johnson, Y-C. Hu, J. Jetcheva, "A performance comparison of Multi-hop wireless ad-hoc networking routing protocols", in the proceedings of the 4th International Conference on Mobile Computing and Networking (ACM MOBICOM '98), October 1998, pages 85-97. (AES). 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
30. Md. Golam Kaosar, Hafiz M. Asif, Tarek R. Sheltami, Ashraf S. Hasan Mahmoud, "Simulation-Based Comparative Study of On Demand Routing Protocols for MANET", available at http://www.lancs.ac.uk
31. Per Johansson, Tony Larsson, Nicklas Hedman, Bartosz Mielczarek, "Routing protocols for mobile ad-hoc networks – a comparative performance analysis", in the proceedings of the 5th International Conference on Mobile, August 1999, pages 195-206.
32. P. Chenna Reddy, "Performance Analysis of Adhoc Network Routing Protocols", Academic Open Journal, SSN 1311-4360, Volume 17, 2006

