On Security Study of Two Distance-vector Routing Protocols for Mobile Ad Hoc Networks *

Weichao Wang, Yi Lu, Bharat K. Bhargava
CERIAS and Department of Computer Sciences
Purdue University
West Lafayette, IN 47907
wangwc, yilu, bb @cs.purdue.edu

Abstract

This paper compares the security properties of Ad Hoc On-demand Distance Vector (AODV) and Destination Sequence Distance Vector (DSDV) protocols, especially the difference caused by on-demand and proactive route queries. The on-demand route query enables the malicious host to conduct real time attacks on AODV. The communication overhead of attacks on DSDV is independent of the attack methods and the width of attack targets. A single false route propagates slower in AODV than in DSDV. The detection of false destination sequence in AODV heavily depends on the mobility of hosts. False distance vector and false destination sequence attacks are studied by simulation. The delivery ratio, communication overhead, and the propagation of false routes are measured by varying the traffic load and the maximum speed of host movement. The anomalous patterns of sequence numbers detected by destination hosts can be applied to detect the false destination sequence attacks.

1. Introduction

The limited power resource and computation capabilities of mobile devices determine their heavy dependence on other hosts for data accessing and information processing. A reliable network topology must be assured through efficient and secure routing protocols for mobile ad hoc networks to enable the pervasive computing.

Many efficient routing protocols for ad hoc networks have been proposed. We may classify them by the time that the routing information is acquired. In the on-demand (reactive) protocols, such as AODV [19], Dynamic Source Routing (DSR) [13], and Temporally Ordered Routing Algorithm (TORA) [17], the routing information is required and maintained only when it is needed. In the proactive protocols, such as Destination Sequence Distance Vector (DSDV) [18], and Clusterhead Gateway Switch Routing (CGSR) [7], the hosts exchange information routinely and construct the routing tables in advance. There are other protocols, such as Zone-based Routing Protocol (ZRP) [9], that employ both mechanisms.

The original versions of the protocols do not consider much on security and robustness. But the routing topology of ad hoc networks is prone to both external and internal attacks in the application environments such as battlefields. Research has been carried out to protect mobile ad hoc networks. The adopted mechanisms include: providing decentralized public key infrastructure [12] [26], distributed monitoring and evaluating host behaviors [14] [22], and using hash chain and digital signature to guarantee the integrity of the information [24] [11] [10]. These methods protect the ad hoc networks from some attacks. However, they face the following difficulties.

- The restrictions on power consumption and computation capabilities prevent the usage of complex encryption algorithms. The time synchronization cannot be efficiently achieved for hash chains.
- The constantly changing topology and dynamic membership increases the difficulty of authentication and key distribution.
- Some attacks cannot be detected by the localized monitoring. Therefore, intrusion detection and intruder identification based on these methods are restricted.

Research is required to ascertain the potential connections between the essential properties of the routing procedures and the security vulnerabilities introduced by them. Then security enhancements addressing these deficiencies

*The research is supported by Center for Education and Research in Information Assurance and Security (CERIAS), NSF grant CCR-0001788, NSF grant ITR-ANI-0219110, and CISCO URP.

can be designed efficiently. This research provides a detailed analysis on security properties of two representative ad hoc routing protocols, namely, AODV and DSDV. We especially examine the difference caused by on-demand and proactive mechanisms. Many examined properties, such as distance vector, and destination sequence, are also adopted by other ad hoc routing protocols. Thus the results can be applied beyond AODV or DSDV and provide guidelines for the design of a secure routing protocol and the Intrusion Detection Systems (IDS) for ad hoc networks.

The remainder of the paper is organized as follows: Section 2 presents the related work. Section 3 presents an overview of AODV and DSDV. Section 4 exploits some attacks on the protocols and compares the security deficiencies caused by on-demand route query and the proactive mechanism. Section 5 illustrates the damages of false distance vector attacks and false destination sequence attacks by simulation. Section 6 presents the anomalous patterns of sequence numbers that can be used to detect false destination sequence attacks. Section 7 concludes the paper.

2. Related work

There are efforts, in both theory analysis and project development, to investigate the security of ad hoc networks, to establish IDS, and to construct secure communication protocols.

Zhang and Lee presented a generic multi-layer integrated IDS structure [25]. But how to efficiently collect the patterns of attacks and how to safely distribute the intrusion detection results to other hosts are not discussed in detail. Bhargavan, Zhou and Haas explored the security issues of wireless LANs and ad hoc networks [26] [5]. They summarized the primary questions to achieve security and the challenges to the routing protocols.

Providing decentralized public key infrastructure is a fundamental problem in securing ad hoc networks. Hubaux and his colleagues proposed a key distribution mechanism similar to PGP [12] [6]. They present a practical solution to the key management problem stated by Haas in [26]. But the transfer of trust among hosts is difficult to apply under some critical environments.

Distributed monitoring and evaluating host behaviors is also popular in security enhancements. A system integrating watchdog and pathrater with DSR is presented in [14]. AODV-S [22] enables the neighbors to collaboratively authorize a token to the host before it can join the activities in the network. But there are attacks that cannot be detected locally and have long delays before the anomaly is discovered. They put challenges on secure information storage and sharing.

Several protocols using hash chain, digital signature or both to guarantee the integrity of routing information have been proposed. [24] uses both mechanisms to protect the routing procedure. SEAD [10] uses one-way hash chains to provide authentication. Ariadne [11] uses a variant of TESLA to achieve similar goals. These protocols may not suffer the attacks exploited in section 4, but the synchronization among mobile devices is not easy to achieve. The evaluation of secure routing in ad hoc networks can be found in [15]. More secure protocols and IDS structures can be found in [20] [23] [16] [1].

3. Description of protocols

3.1. Introduction of DSDV

DSDV is based on distance vector technology. Every host broadcasts its routing table routinely, which enables the proactive route discovery. When one link change that may severely impact the connectivity happens, a partial update can also be sent. To avoid the routing loop, DSDV uses the destination sequence number to identify the freshness of the routing information. The sequence number of a specific host is increased at every time when it sends out the route update. The route with the largest sequence number is always preferred. When multiple paths with the same sequence are available, the shortest one will be selected. More details about DSDV can be found in [18].

DSDV's desirable feature is the short delay of connections brought by proactive route discovery. Because every host has to maintain a routing table that covers all hosts, DSDV does not scale well to large networks. The overhead of recalculation of routes and periodical packet exchanges consume the valuable resources of energy and bandwidth. However, the proactive mechanism sets up difficulties for the malicious hosts to conduct attacks. This will be shown by the analysis and simulation results presented later.

3.2. Introduction of AODV

AODV is a reactive protocol and it is based on distance vector technology. When the source host wants to send packets to the destination and cannot get the route from its routing table, it will broadcast a Route Request (RREQ). The receivers may establish the routes back to the source host through the RREQ. If the receiver has an active route to the destination, it will unicast a Route Reply (RREP). Otherwise, the RREQ will be re-broadcast further. If a reply is sent, all hosts along that path may establish the route to the destination. To prevent the same request from being broadcast repeatedly, every request is identified by a <Host ID, Broadcast ID> couple. The mobile hosts send out the Route Error (RERR) packets to report broken paths.

To avoid routing loop and to identify the freshness of the route, destination sequence number is introduced. The

sequence of a mobile host is increased at every time that it sends RREQ or RREP. The sequence in RREP must be larger than or equal to the one carried in corresponding RREQ. The path with the largest destination sequence number is always preferred. If several paths have the same sequence, the shortest one will be chosen. More details about AODV can be found in [19].

AODV's desirable features are its low byte overhead and loop free routing. But the on-demand route query usually brings a longer delay for the first few packets. The genuineness of the destination sequence and distance vector leaves vulnerabilities to attackers. These deficiencies introduce the attacks that will compromise the network.

4. Attack analysis and security comparison

We exploit some attacks on AODV and DSDV to expose the potential linkage between the essential features of the protocols and their security flaws. The primary difference between AODV and DSDV is that they work in on-demand and proactive modes separately. It leads to the difference in the conduction costs of attacks, propagation procedures of false routes, and the detection of attacks.

4.1. Classification of attacks

We first divide the attacks into passive and active categories. At a finer level, we group the active attacks by their target features.

4.1.1. Passive attacks. A malicious host conducts a passive attack by ignoring operations supposed to be accomplished by it. One example of passive attacks on AODV or DSDV is silent discard, carried on by an intermediate host along the forwarding path. Instead of forwarding a packet to the next hop, the attacker drops the data silently. Another example is partial routing information hiding. It is conducted by a malicious host in DSDV by hiding the available paths to specific hosts when it broadcasts its routing table, or in AODV by ignoring to give out RREP when an active route is available.

It is usually difficult to distinguish passive attacks from Byzantine failures [2] in ad hoc networks. For example, a packet drop can also occur because of host movement or unreliable wireless media. Fortunately, the constantly changing topology and multiple available paths among hosts limit the impacts of passive attacks. For example, our simulation shows that [21] in an ad hoc network that has 30 hosts and 25 connections, the silent discard by one malicious host may cause the delivery ratio to decrease 3%. We do not put more efforts on the analysis of passive attacks because they rely more on the network topology than the protocol characteristics.

4.1.2. Active attacks. The malicious host generates an active attack by introducing false information into an ad hoc network. It confuses routing procedures and degrades network performance. In DSDV the false information is carried in the routing packets. In AODV, the RREP is especially attractive to attackers because the reverse routes established by RREQ will become expired in a short time if no active traffic uses those routes. Two active attacks that threat both AODV and DSDV are:

- False distance vector attack

In both AODV and DSDV the hosts collect routing information solely from direct neighbors. The incomplete understanding of global topology enables the false distance vector attacks. The malicious host can claim that the destination is one (or a few) hop(s) from it in the routing update packets or RREP even if it does not have any available path in its routing table. If no other replies provide a fresher or shorter route, the source will choose the path provided by the malicious host, and the data packets will be dropped or compromised.

- False destination sequence attack

Both AODV and DSDV employ destination sequence to identify the freshness of routing information. When multiple routes are available, the source host always chooses the one with the largest sequence number. By assigning a large false destination sequence in the routing update packets or RREP, the attacker's reply can easily beat other replies and attracts the data traffic. Even worse, the deceived hosts will propagate in good faith the false route to other hosts, thus strengthening the impacts of the attack.

4.2. Security analysis

4.2.1. Security comparison. The primary difference between AODV and DSDV is the adoption of on-demand and proactive methods separately. Each of the methods brings advantages and disadvantages in security. While the on-demand route query enables low protocol overhead and adaptability to host movement, it also leaves a lenient space to the attackers. In proactive protocols the malicious host can send multiple false routes in the same packet. The detailed comparison on security comes as follows:

The on-demand property enables the malicious hosts to conduct real time attacks. Most of the attacks on AODV do not need any preparation or establishment time. For example, when a malicious host receives a RREQ, it can immediately form a false route reply and conducts the attack. As a comparison, when the malicious host attacks a proactive protocol, it must send out the false information in advance

and has to routinely update the fake route to keep it alive. The longer a false route exists, the larger probability that it is detected. At this point, it is difficult to catch an on-going attack on a reactive protocol before it causes performance degradation.

The on-demand property enables the attackers to make flexible choices on the targets, the methods, and the points in time of attacks. For example, the malicious host can choose to attack all connections to or from a specific host. It can attack the same host with different methods. As to one victim, the attacker can choose to send false replies to some of the route queries while leaving others untouched. As a comparison, an attack on a proactive protocol usually does not have the flexibility. For example, a false route with a large sequence will be propagated to all other hosts through route exchanges. It is difficult for the malicious host to attack a specific connection without impacting others. This stiffness increases the probability that the attacker is detected and located.

It is more difficult to trace back the sources of false information in AODV. The routing reply is unicasted back to the source. Unless the mobile hosts monitor all nearby traffic, there will be only one host along the false route that directly receives the false information from the attacker. For the intruder identification algorithms that use quorum voting to locate the attacker [21], AODV is less efficient on the trace back procedures.

4.2.2. Communication overhead of attacks. The communication overhead caused by sending false routes in AODV is determined by the width and frequency of attacks. For example, if the malicious host wants to attack one specific connection, it only needs to send a single false RREP. As the other extreme condition, if the malicious host wants to attack every connection to every other host, it has to send many false RREP. In DSDV, the overhead is more consistent. The attacker can send many false routes in the same routing packet. At this point, attacking proactive protocols is more communication efficient for an aggressive attacker.

4.2.3. Propagation of false routes. In AODV, the false RREP will be unicasted back to the source host. In [8] it has shown that the average path length is proportional to the square root of host density in ad hoc networks. Therefore the number of hosts cheated by a false RREP is proportional to that order. Because an intermediate host may send out RREP to other route queries afterwards, the false routes will form a tree rooted at the malicious host. In a proactive protocol, the false routes will be transmitted within a growing round area by the routing exchanges. At this point, a single false route in AODV propagates slower and has weaker impacts.

4.2.4. Cancellation of false routes. As the IDS in ad hoc networks develop, the malicious host sometimes has to cancel the false routes originated from it to avoid being identified. In most ad hoc routing protocols, the updates to current routes are caused either by the break of an active link or the appearance of a fresher or shorter path. The attacker in DSDV can stop sending false routes to cancel the impacts. The new updates will be propagated to the neighbors and the false routes will be smoothly replaced. The number of hosts that notice this change depends on the propagation range of the false routes. In AODV, when the attacker stops sending packets, the neighbors will assume that the link is broken. The re-discovery procedure will broadcast RREQ. At this point, it is more difficult for the attackers in AODV to silently cancel the impacts of false routes.

4.2.5. Detection of false routes. It is difficult to detect false distance vector attacks in AODV and DSDV because the hosts cannot construct the global view of the connectivity. The false destination sequence attacks can be detected by the victim if it finds that the sequence has never be generated by it. Because in DSDV the hosts routinely exchange their routing tables, we can estimate the maximum propagation delay of the false sequence from the attacker to the victim by the product of routing packet broadcast interval and their distance in hops. If the false sequence outruns the real number when it arrives at the victim, the attack will be detected. In AODV, the false sequence can be detected only when the false path is broken and the re-discovery procedure broadcasts a RREQ carrying the false number. It depends on the mobility of the hosts and no upper limit can be predicted. More details about the detection of false sequence attacks will be discussed in section 6.

5. Simulation results

We study the practical impacts of the attacks and examine our analysis through simulation. Two attacks on AODV and DSDV are considered: false distance vector and false destination sequence. Except sending false routes, the attacker will discard any data packets passing through it. Two traffic conditions are tested. Under condition one, all connections have the same destination. This condition is chosen to simulate the scenario in which the malicious host only attacks the hot point in the applications and tries to block traffic to it (e.g. block soldier's reports to officer, or sensor's reports to information-sink). We measure the delivery ratio, attack overhead, and the propagation of false routes when the malicious host sends false routes about the common destination. Under condition two, a more sophisticated traffic scenario is used. We study the delivery ratio and attack overhead against the mobility of the hosts.

The simulation of attacks is deployed using ns2. Table 1

lists the simulation parameters that we use.

Table 1. Simulation parameters

Simulator	ns-2
Examined protocols	AODV, DSDV
Simulated attacks	False distance vector, False destination sequence
Simulation duration	1000 seconds
Simulation area	1000 * 1000 m
Number of mobile hosts	30
Transmission range	250 m
Movement model	Random waypoint
Maximum speed	5 – 20 m / s
Traffi c type	CBR (UDP)
Data payload	512 bytes
Packet rate	2 pkt / s
Number of malicious host	1
Host pause time	10 seconds

The choices of the parameters consider both accuracy and efficiency of the simulation. The host moving speed covers a range from human jogging to vehicle riding in country field. Faster speed is not considered because the frequency of route changes will confuse the performance degradation caused by attacks. The packet rate is chosen to avoid congestion even when there are multiple connections converging at the same host.

We choose the following metrics to evaluate the impacts of attacks: (1) packet delivery ratio (2) false routing packets sent by the attacker (3) the number of normal hosts that are cheated by the false routes.

Metric (1) is selected to evaluate the percentage of packets that are affected by the attacks. This can be viewed as the "strength" of an attack. Metric (2) is used to examine the communication overhead of different attacks. Metric (3) examines the propagation of false routes and the potential impacts that are not shown by metric 1. Combining metric 2 and 3, we can examine the efficiency of the attacks.

5.1. Simulation condition one

Under condition one, all connections have different sources and use node 29 as the destination. Node 5 is the malicious host. In AODV, it sends false RREP to every RREQ that it receives. In DSDV, it sends false routing information about node 29 in the route update packets. We study the selected parameters against the number of connections. Because there are thirty hosts in the network, the maximum number of connections from different sources to node 29 is twenty-eight (except node 5 and 29). The maximum speed of host movement is 5m/s. Every point in the figures is the average value of ten simulation scenarios. To calculate the number of hosts getting cheated by the false routes, the routing trees to node 29 are examined every 50 seconds. Figure 1, 2, 3 and 4 show the simulation results.

Figure 1 shows the delivery ratio versus the number of connections to node 29 under three conditions in both protocols: when node 5 does not conduct attacks, when it attacks the routes with false distance vector, and when it attacks with false destination sequence. It is easy to tell that the impact of false destination sequence attack on delivery ratio is much more severe than that of false distance vector attack. The reason is that both AODV and DSDV prefer fresh routes to short ones.

Considering the delivery ratios under false distance vector attacks, we find that in both protocols they drop to around 50% to 60%. It is determined by the characteristic of distance vector mechanism. If the attacker can accurately predict the sequence number of node 29, the probability that a host will be cheated depends on the probability that it is closer to the attacker than to the victim. In this test environment, it is 50% because the movement of every host is independent. Because the attacker applies a conservative method to predict the sequence number of the victim, the delivery ratio is a little higher than 50%.

The difference between the delivery ratios of ADOV and DSDV when they are under false destination sequence attacks is caused by the implementation of the attacker behaviors. In AODV, the malicious host will add a constant value to the sequence number carried in corresponding RREQ and uses the result as the sequence in false RREP. We choose the constant as 2 in the simulation. So there are chances that the false sequence cannot beat the real number. In DSDV, once the false sequence has been established, the false route propagates throughout the network. So more hosts will be cheated. If in AODV the attacker uses a very large number as the false sequence (e.g. 0x7fffffff), we would expect a lower delivery ratio.

One interesting point, when AODV is under attacks on destination sequence, is that the delivery ratio will increase a little as the number of connections increases. It happens because the attacker only adds a constant to the sequence in RREQ. As the number of connections increases, the true sequence increases faster, and the probability that the chosen fake sequence is smaller than the real value also increases. Thus less traffic will be attracted to the attacker.

Figure 2 shows the number of hosts that are cheated by the false routes versus the number of connections. In DSDV, the number of hosts that are cheated does not vary a lot as the number of connections changes because of the proactive property. When false distance vector attacks are conducted, less than half of the hosts are cheated. But when the network is under false destination sequence attacks, almost all hosts are cheated. In AODV, as the number of connections increases, more false RREP will be sent by the attacker. Therefore, more normal hosts will be cheated. Both protocols prefer the route with larger sequence, so the false destination sequence attacks cheat more hosts. If the hosts are

uniformly distributed in the test area, there are about half of the hosts that are closer to the attacker than to the destination. They will be cheated by the false distance vector attacks if the sequence numbers in false routes are the same as the real ones. Because the attacker applies a conservative sequence prediction method, there are less than 50% of the hosts that are cheated in both protocols.

Figure 3 shows the communication overhead of the two attacks. The number of false route updates sent in DSDV does not change a lot because of the proactive property. And the overhead of conducting two attacks does not show big difference. In AODV every false RREP can only attack one RREQ, so the number of false RREP sent by the attacker is roughly proportional to the number of connections. The two curves for AODV are very close to each other, which shows that both attacks put similar traffic overhead on the attacker. But the one for false destination sequence attacks is a little higher. It is because the false sequence numbers generated by the attacker disturb the updates to real numbers and introduce more route queries into the system.

Figure 4 examines the efficiency of the two attacks in both protocols. It shows the number of hosts got cheated versus the number of false route packets sent by the attacker. For DSDV, the values form two group of points which are very close to each other. They can be derived from the curves shown in figure 2 and 3. For AODV, the curves are very similar to the lines in figure 2 because the number of false RREP sent by the attacker is roughly proportional to the number of connections.

From figure 1 to figure 4, we can tell that the attacks on destination sequence and the attacks on distance vector have similar communication overhead but the former ones have more severe impacts. For the intrusion prevention and intrusion detection systems designed to protect ad hoc networks using AODV or DSDV, this kind of attack should be considered first.

5.2. Simulation condition two

Under condition two, we generate a scenario that contains twenty-nine connections. Each normal host is the source of one connection and the destination of another. Node 5 sends false routes about all other hosts. We study the selected parameters versus the mobility of the hosts, which is represented by the maximum moving speed.

Figure 5 shows the delivery ratio versus the maximum speed of hosts under the conditions the same as figure 1. The delivery ratio of attack free AODV keeps high, which shows that the mobility of host is still within the suitable serving range of AODV. DSDV has a slower response to link changes caused by host movement, so the delivery ratio decreases faster. When the malicious host conducts false destination sequence attacks on DSDV, the false routes will

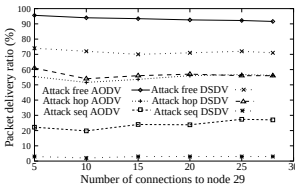

Figure 1.

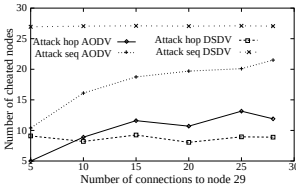

Figure 2.

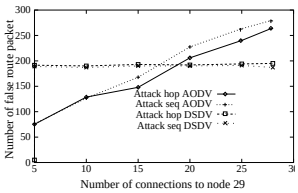

Figure 3.

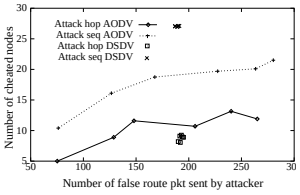

Figure 4.

Figure 1–4. Simulation results for condition one.

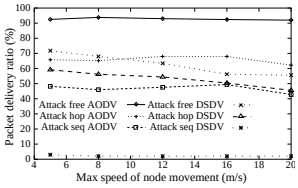

Figure 5.

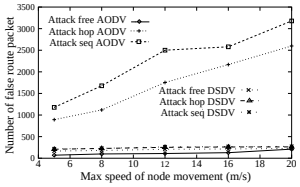

Figure 6.

Figure 5–6. Simulation results for condition two.

propagate throughout the network. Most of the normal hosts will be cheated. So the delivery ratio will be low. Comparing to figure 1, we find that more data packets successfully reach to the destinations when AODV is under attack. This can be explained by the difference between the connection scenarios of the two test cases. Under condition two, every host is the source of one connection, and it may broadcast the RREQ throughout the network. Other hosts can establish the routes through the paths that they receive the request. Therefore, many hosts do not have to listen to the false RREP sent by the attacker. More safe routes are set up and the delivery ratio is higher.

Figure 6 shows the number of routing packets sent by node 5 when it behaves properly and when it conducts the attacks. In DSDV, the curves are very close to each other because the attacker can carry multiple false routes in the same routing packet. It does not have to increase the frequency of sending route updates. In AODV the attacker will send five to ten times more RREP when it attacks every RREQ it receives. It is not efficient for an aggressive malicious host to attack all connections at the same time in a reactive protocol. This anomalous increase may also be detected by IDS. Further research is required on the behaviors of intelligent attackers and suitable responses.

6. Detecting false destination sequence attacks

When the malicious hosts introduce false information into the networks, their behaviors and the conflicts between false and true information form special patterns, which can be used to detect the attacks. In addition, the connectivity history and the propagation paths of the false information can be used to identify the sources of attacks. Our research on security in ad hoc networks [21] tries to collect patterns of attacks and to provide guidelines for the design of the IDS. An example of detecting false destination sequence attacks in AODV and DSDV is given out below.

False destination sequence attacks can cheat a large part of the hosts and severely impact the delivery ratio. To "beat" other available routes, the attacker must choose a number, which is larger than the sequence generated by the real destination, as the false sequence to show its "freshness". If the victim host can find this false sequence number, it will detect the attack. In DSDV the false sequence route will be transferred to all directions. There exists an upper limit of delay that the false route will reach to the victim if it is connected to the attacker and the false sequence always outruns the real one. In AODV, only when a host on the false route moves out of the range of its neighbor, the re-initiation procedure of the source will send out RREQ that carries the false sequence. Because the RREQ is broadcast throughout the network, there is a good chance that the real destination will receive the request. If the false sequence is still larger than the real one, the host detects the attack. Therefore, no upper limit of delay between the attack is conducted and it is detected can be guaranteed.

The sequence number of a host is carried in the routing packets. Under the normal operation of AODV and DSDV, the sequence carried in the packets can never be larger than the real sequence plus one. But when the host is under false destination sequence attacks, the difference between the received and local sequence numbers can be larger than or equal to 2. Figure 7 and 8 show the difference between the two sequence numbers detected by a host when all other hosts behave properly and when one malicious host attacks it with false destination sequence. In DSDV, when the false sequence is larger than the real number, it can be detected in any route update sent by a neighbor of the victim. If the real number is larger, the attacker will find it and conducts the new attack. Therefore the difference fluctuates between 0 and 2. In AODV, the normal host detects eleven times that the incoming sequence number is larger than local number plus one.

In both scenarios some attacks are not detected. Two problems that impact the detection of false destination sequence attacks on AODV and DSDV are: (1) The real sequence may outrun the false one when it is received by the victim. (2) A tight limit of the delay between the

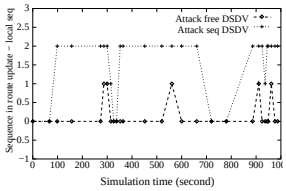

Figure 7.

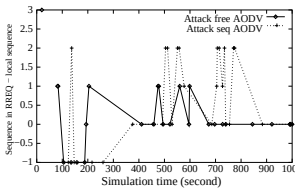

Figure 8.

Figure 7–8. Anomalous patterns of sequence.

false sequence is generated and it reaches the victim, if the two hosts are connected, should be achieved. A protocol that uses one detected attack to activate the detection of other attacks has been designed [21]. The basic idea is to re-examine all routing information coming from the same sources and activate the re-initiation. A software module that can be integrated into AODV and DSDV to improve the detection accuracy is under construction.

Collecting and determining the anomalous patterns of attacks is a challenging topic in IDS for ad hoc networks. The example provided above shows that combining protocol analysis and practical simulation may accelerate this procedure.

7. Conclusions

The security of the ad hoc network routing protocols is still an open problem and deserves more research work. This paper studies the vulnerabilities of and attacks on two protocols – AODV and DSDV. The analysis shows that as AODV provides fair performance with reasonable overhead and adaptability to both traffic load and host mobility, the on-demand property also introduces some security deficiencies. It allows the malicious host to attack the network in real time with flexibility. It is more difficult to locate the sources of the false information. The proactive property also has disadvantages. The routine exchange of routes enables the false routing information to propagate within a wider range. The malicious host can conduct multiple attacks in the same routing packet. Because both protocols prefer the fresh routes which are identified by large sequence numbers, the attacks on destination sequence have more severe impacts than the attacks on distance vector.

The simulation supports our analysis. The delivery ratio curves show that the attacks on destination sequence will attract more packets to the attackers. False distance vector attacks will cheat less than 50% of the hosts in a uniformly distributed network. The communication overhead caused by conducting attacks is more stable on the traffic load and the width of attacks in DSDV than in AODV. The analysis and simulation also show that it is more efficient to detect false destination sequence attacks in DSDV than in AODV.

The research to protect wired network routing protocols [3] has shown that it is the property, instead of the protocol detail, that leads to the security deficiencies. The example attacks on AODV and DSDV can also be applied to attack other protocols sharing the properties. Thus the analysis results and anomalous patterns of the attacks can be employed to prevent or detect the coterminous attacks on different protocols. Because the primary difference between AODV and DSDV is the on-demand and proactive properties, we may generalize the analysis to other on-demand or proactive protocols.

There are many problems to be solved in protecting the ad hoc networks. We plan to study the relationship between the average delay of detecting false destination sequence attacks and the mobility of the hosts. We will design an efficient mechanism which can establish safe routes when false routing information is discovered. We plan to study more features of the routing protocols to exploit their security deficiencies. On achieving the secure distribution of individual intrusion detection result, we plan to establish the trust relation among hosts in the open area of ad hoc networks [4]. The results will provide the guidelines for the design of a secure ad hoc routing protocol and become the building blocks of the IDS for ad hoc networks.

References

[1] P. Albers and O. Camp. Security in Ad Hoc network: A general ID architecture enhancing trust based approaches. In *Proceedings of International Conference on Enterprise Information Systems (ICEIS)*, 2002.

[2] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens. An on-demand secure routing protocol resilent to Byzantine failures. In *Proceedings of ACM Workshop on Wireless Security (WiSe)*, 2002.

[3] S. Bellovin. Security problems in the TCP/IP protocol suite. *Computer Communications Review*, 19(2):32–48, April 1989.

[4] B. Bhargava and Y. Zhong. Authorization based on evidence and trust. In *Proceedings of Data Warehouse and Knowledge Management Conference (DaWak), France*, 2002.

[5] V. Bharghavan. Secure wireless LANs. In *Proceedings of the ACM Conference on Computers and Communications Security*, 1994.

[6] S. Capkun, L. Buttyan, and J.-P. Hubaux. Self-organized public-key management in ad hoc wireless networks. In *Proceedings of ACM Workshop on Wireless Security (WiSe)*, 2002.

[7] C. Chiang. Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel. In *Proceedings of IEEE SICON*, 1997.

[8] M. Grossglauser and D. Tse. Mobility increases the capacity of Ad-hoc wireless networks. In *Proceedings of INFOCOM*, 2001.

[9] Z. Haas and M. Pearlman. The zone routing protocol (ZRP) for Ad Hoc networks. IETF Internet Draft, Version 4, July, 2002.

[10] Y. Hu, D. Johnson, and A. Perrig. Sead: Secure efficient distance vector routing for mobile wireless ad hoc networks. In *Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA)*, 2002.

[11] Y. Hu, A. Perrig, and D. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. In *Proceedings of ACM MobiCom*, 2002.

[12] J. Hubaux, L. Buttyan, and S. Capkun. The quest for security in mobile ad hoc network. In *Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*, 2001.

[13] D. Johnson, D. Maltz, and J. Jetcheva. *DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Network*. Ad Hoc Networking, Addison-Wesley, 2001.

[14] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the Sixth annual ACM/IEEE International Conference on Mobile Computing and Networking*, 2000.

[15] P. Papadimitratos and Z. Haas. Performance evaluation of secure routing for mobile ad hoc networks. In *Proceedings of ACM Workshop on Wireless Security (WiSe)*, 2002.

[16] P. Papadimitratos and Z. Haas. Secure routing for mobile Ad Hoc networks. In *Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS)*, 2002.

[17] V. Park and M. Corson. A highly adaptable distributed routing algorithm for mobile wireless networks. In *Proceedings of IEEE InfoComm*, 1997.

[18] C. Perkins. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In *Proceedings of SIGCOMM*, 1994.

[19] C. Perkins and E. Royer. Ad-Hoc On-Demand Distance Vector Routing. In *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, 1999.

[20] P. Sinha, R. Sivakumar, and V. Bharghavan. Enhancing Ad-Hoc routing with dynamic virtual infrastructures. In *Proceedings of IEEE INFOCOM*, 2001.

[21] W. Wang, Y. Lu, and B. Bhargava. Intruder identification in ad hoc on-demand distance vector protocol. Technical report, Department of Computer Sciences, Purdue University, 2002.

[22] H. Yang, X. Meng, and S. Lu. Self-organized network-layer security in mobile ad hoc networks. In *Proceedings of ACM Workshop on Wireless Security (WiSe)*, 2002.

[23] S. Yi, P. Naldurg, and R. Kravets. Security-aware ad hoc routing for wireless networks. Technical report uiucdcs-r-2001-2241, Department of Computer Science, University of Illinois, Urbana-Champaign, 2001.

[24] M. Zapata and N. Asokan. Securing ad-hoc routing protocols. In *Proceedings of ACM Workshop on Wireless Security (WiSe)*, 2002.

[25] Y. Zhang and W. Lee. Intrusion detection in wireless Ad-Hoc networks. In *Proceedings of ACM MobiCom*, 2000.

[26] Z. Zhou and Z. Haas. Securing Ad Hoc networks. *IEEE Networks*, 13(6):24–30, 1999.