ON VULNERABILITY AND PROTECTION OF AD HOC ON-DEMAND DISTANCE VECTOR PROTOCOL

by Weichao Wang, Yi Lu, Bharat K. Bhargava

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907-2086

On Vulnerability and Protection of Ad Hoc On-demand Distance Vector Protocol

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

Abstract— **Vulnerabilities and the attacks on Ad Hoc On-demand Distance Vector (AODV) protocol are investigated and studied via analysis and simulation. The attacks are classified by their target properties. The analysis shows that the on-demand route query enables the malicious host to conduct real time attacks on AODV. False distance vector and false destination sequence attacks are studied by simulation. Two connection scenarios: common destination and uniformly distributed traffic load are considered. The delivery ratio, attack overhead, and the propagation of false routes are measured by varying the number of connections and the mobility of the hosts. The simulation results illustrate that the attacker can confuse the network connectivity with false routes and lead to a decrease up to 75% in the delivery ratio. When the hosts are uniformly distributed, the false distance vector attacks can not cheat more than half of the hosts. But the false destination sequence routes can propagate to most of the network. The anomaly patterns of sequence numbers carried by routing request (RREQ) can be applied to detect the false destination sequence attacks. The vulnerability analysis results and anomaly patterns can be employed by other Ad Hoc routing protocols to establish intrusion prevention and detection mechanisms.**

Index Terms— **Ad Hoc Networks, AODV, Vulnerability, Intrusion Detection.**

I. Introduction

A mobile Ad Hoc network is a collection of wireless hosts that can be rapidly deployed as a multi-hop packet radio network without the aid of any established infrastructure or centralized administration [1]. Such networks can be used to enable next generation of battlefield applications envisioned by the military [2], including situation awareness systems for maneuvering war fighters, and remotely deployed unmanned micro-sensor networks. Ad Hoc networks can provide communication for civilian applications, such as disaster recovery and message exchanges among medical and security personnel involved in rescue missions.

The mobile devices usually have limited storage and low computational capabilities. They heavily depend on other hosts and resources for data access and information processing. A reliable network topology must be assured through efficient and secure routing protocols for Ad Hoc networks.

Many efficient routing protocols for Ad Hoc networks have been proposed. We may classify them by the timing of acquisition of routing information and the methods by which the routes are maintained. In the on-demand (reactive) protocols, such as AODV [3], Dynamic Source Routing (DSR) [4], and Temporally Ordered Routing Algorithm (TORA) [5], the routing information is required and established only when it is needed. In the pro-active protocols, such as Destination Sequence Distance Vector (DSDV)[6], Clusterhead Gateway Switch Routing (CGSR) [7], and Wireless Routing Protocol (WRP) [8], the hosts exchange the 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. A number of studies on performance comparison and optimization for these protocols in an attack-free environment have been published [10], [11], [12], [13]. The performance parameters include delivery ratio, packet delay, protocol overhead, and throughput. They are measured by varying the input parameters such as host mobility, host density, and traffic load.

Current Ad Hoc routing protocols assume that the mobile hosts in the Ad Hoc networks will behave properly and will not introduce malicious information into the systems. However, considering the environments (battlefields, disaster rescue, etc.) in which Ad Hoc networks operate, the routing topology is prone to both external and internal attacks by malicious hosts. Research has been carried out to update and apply the security methods in wired networks to the Ad Hoc environments [14], [15]. These include information encryption and user authentication. But these methods face the following difficulties:

- The restriction on power consumption and the limited computational capability of mobile devices prevent the use of complex encryption algorithms.
- The constantly changing network topology increases the difficulty and overhead of authentication. The dynamic membership adds challenges on the key distribution and management.
- These methods can only guard against external attacks. But the internal attacks coming from compromised hosts have severe impacts on network performance and connectivity.

The security and safety characteristics of Ad Hoc routing

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

The paper is accepted to appear in the proceedings of ICT 2003

protocols are different from those in wired networks. Research is required for the vulnerabilities of the protocols, the possible attacks, and their impacts on the network performance.

This research presents a detailed analysis of vulnerabilities and the simulation of attacks on one of the Ad Hoc routing protocols. We choose AODV as the research object. Many methods adopted by AODV, such as on-demand route query, distance vector, destination sequence, and link change reports, are also used by other Ad Hoc routing protocols. The research enables us to ascertain the potential connections between the vulnerabilities and these methods.The results can be applied beyond AODV and provide guidelines for the design of attack prevention mechanisms and the Intrusion Detection Systems (IDS).

The remainder of this paper is organized as follows: Section II presents the related work. Section III presents an overview and characterization of AODV. Section IV exploits the vulnerabilities of and attacks on AODV. It classifies the attacks by their target properties and especially studies the security deficiencies caused by on-demand route query. Section V illustrates the damages in practical settings. It collects the impacts of false distance vector attacks and false destination sequence attacks by simulation. We find that a considerable part of the hosts are cheated by the false routes and it may drastically lower the delivery ratio. The communication costs of the attacks against the network traffic load and host mobility are studied. Section VI presents the anomaly patterns of sequence number that can be used in the detection of false destination sequence attacks. Section VII concludes the paper.

II. Related Work

Research in both theoretical analysis and project development is underway to investigate the security of Ad Hoc networks and to establish IDS. The efforts in securing communication for wireless networks are also relevant to our work.

Zhang and Lee studied the security characteristics of Ad Hoc networks. They identify the difficulties in applying current IDS to the wireless environments [16]. They presented a generic multi-layer integrated IDS infrastructure for the Ad Hoc networks. But solutions to some critical problems remain. How to efficiently collect the patterns of attacks and how to safely distribute the intrusion detection results to individual host need further research. Bhargavan, Zhou and Haas explored the security issues of wireless LANs [17] and Ad Hoc networks [18]. They summarized the primary problems to achieve security and the challenges to the routing protocols.

Several protocols have been established to protect the network layer in a mobile Ad Hoc network. The researchers at UCLA have built a self-organized network-layer security mechanism to enable the neighbors to monitor the behaviors of a specific host [19]. Hubaux and his colleagues established a public key management mechanism in mobile Ad Hoc networks [20]. It presents a practical solution to the key management problem stated by Haas in [18]. The evaluation of secure routing in Ad Hoc networks can be found in [21]. Other security analyses and IDS structures have been presented in [22], [23], [24], [25]. But no security comparisons based on quantitative results have been reached.

Several projects are underway to develop secure communication or build IDS for Ad Hoc networks [2], [26], [27], [28]. The technologies include sending data through multipath to increase reliability, and monitoring traffic distribution to avoid DoS attacks. These will increase both computation and communication overhead during the normal operation period and affect the network performance.

III. Description of AODV

AODV is a reactive protocol that determines routes solely on-demand. It is based on the distance vector technology. The hosts only know the next hop to every destination. When a source host wants to send packets to the destination and cannot get the routes from its routing table, it will broadcast a Route Request (RREQ). The receivers may establish the routes back to the source host through the paths that they get the RREQ. If the receiver has an active route to the destination, it will unicast a Route Reply (RREP) back to the source. Otherwise, the RREQ will be re-broadcast further. If a reply is sent, all hosts along that path may record the route to the destination through this packet. Because there may exist multiple exclusive paths between two hosts, a mobile host can receive the same RREQ more than once. To prevent the same request from being broadcast repeatedly, every request is uniquely identified by a <Host ID, Broadcast ID> couple. Every host keeps a record for the RREQs that have been processed. The mobile hosts send out the Route Error (RERR) packets to their neighbors to report broken paths and activate the route re-discovery procedure.

To avoid routing loop and identify the freshness of the route, destination sequence number is introduced. The sequence number of a mobile host can only be updated by itself in monotonically increasing mode. A larger sequence number denotes a fresher route. The sequence number is carried in both RREQ and RREP. The sequence number in RREP must be larger than or equal to the one carried in corresponding RREQ to avoid the source host to adopt a stale path. When more than one path represented by different RREPs is available, the one with the largest destination sequence number is used. If several paths have the same sequence number, the shortest one is chosen. More details about AODV can be found in [3].

AODV's desirable features are its low byte overhead in relatively static networks and loop free routing using the destination sequence numbers. There are improvements in AODV to support multicast [29] and to detect/maintain multiple paths [30]. But the on-demand route query usually brings longer delay for the first few packets. It suffers from the problems of route request flooding and the use of

MAC level broadcast. The genuineness of the destination sequence and distance vector leaves it vulnerable to attackers. These problems introduce the attacks described next.

IV. Attacks on AODV

The security deficiencies of AODV make it vulnerable to attacks. 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. Another hot target of attacks is the broadcast feature of routing query. If not handled properly, the flood of queries will exhaust the valuable bandwidth. We examine the conduct procedures of the attacks. Their impacts and the propagation of the false routes are also studied.

A. Classification of attacks

The attacks can be classified in different ways. They can be based on the sources of the attacks (internal attack, external attack), or on the methods through which the attackers acquire control (e.g. buffer overflow, Trojan Horse). Others use the targets (e.g. file access control, network connectivity). We divide them into passive and active attacks. At a finer level, we categorize the active attacks on AODV by their target features.

1) Passive attacks: A malicious host conducts a passive attack on Ad Hoc networks by ignoring operations required from it. The attacker does not actively initiate malicious actions to cheat other hosts. One example of passive attacks on AODV is silent discard that is carried on by an intermediate host along the routing path. Instead of forwarding a packet to the next hop, the attacker drops the data silently. Another example of passive attacks is partial routing information hiding. It is conducted by a malicious host by not sending out RREP when an active route is available.

It is usually difficult to distinguish passive attacks from Byzantine failures [31] [32] in Ad Hoc networks. For example, a message loss can also occur because of host movement or unreliable wireless media. Fortunately, the constantly changing topology and multiple available paths between hosts limit the impacts of passive attacks. For example, in an Ad Hoc network having 30 hosts and 25 connections, the silent discard by one malicious host may cause the delivery ratio to decrease by 3%. The analysis and detection of passive attacks is not discussed further because such attacks rely more on the network topology than the protocol characteristics.

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. Three examples of active attacks on AODV are: false distance vector, false destination sequence, and vicious query flooding.

AODV is based on the distance vector technology and the hosts collect routing information from immediate neighbors. The incomplete knowledge of the global topology enables the false distance vector attacks. The malicious host forms this attack by claiming that the destination is one (or a few) hop(s) from it in the RREP packet even if it does not have any available path in its routing table. If no other replies provide a better route, the source will choose the path provided by the malicious host. The data packets will be dropped or compromised by the attacker.

AODV employs destination sequence number 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 number in RREP, the attacker's reply can easily supersede other replies and attracts the data traffic. Even worse, the deceived hosts will propagate in good faith the false route to other hosts and exacerbate the impacts of the attack.

Vicious query flooding targets at bandwidth consumption. AODV uses broadcast during the route discovery procedure. The malicious host may choose a non-exist address as the destination and sends out the RREQ packets at high frequency. The RREQ packets will flood the Ad Hoc network because no host can give a reply. The flood will delay the transmission of other traffic and increase the packet drop ratio, thus lowering the performance of the network.

B. Security analysis

1) Security weak points: While the on-demand property of AODV enables its advantages on low protocol overhead and adaptability to host movement, it is lenient to the attackers. It has the following disadvantages on security:

The on-demand property of AODV 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 source host broadcasts RREQ in the network, the malicious host may immediately form a false route reply and execute the attack. As a comparison, when the malicious host tries to attack a pro-active 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, larger the probability that it is detected. It is difficult to catch an on-going attack on AODV before it causes performance degradation.

The on-demand property of AODV enables the attackers to have multiple choices of the targets and points in time of attacks. For example, the malicious host can choose to attack the RREQ coming from a specific source, or it may choose to attack all connections to a particular destination. It can attack the same host with different methods. As to one victim, the attacker can send false replies to some of the routing queries while leaving others untouched. By comparison, the false route in a pro-active protocol usually has fixed object and fixed type of attack. This increases the probability that the attacker is detected and located.

It is more difficult to trace back the sources of the false information in AODV than in a pro-active protocol. As discussed earlier, the attacks on AODV focus on the RREP packets. 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 suspicious attacker [33], AODV is less efficient on the trace back procedures.

2) Propagation of false routes: In AODV, the false RREP will be unicasted back to the source host. In [34] it has been shown that the average path length is proportional to the square root of host density in Ad Hoc networks. Therefore the number of hosts immediately cheated by a false RREP is proportional to that order. Since an intermediate host may send out RREP to other route query afterwards, the false routes will form a tree rooted at the malicious host. In a pro-active protocol, the false routes will be transmitted to a growing surrounding area by the routine exchanges of routing information until they are replaced by better routes. A single false route in AODV propagates slower and has weaker impacts.

3) Cancellation of false routes: As the intrusion detection systems in Ad Hoc networks develop, the malicious host sometimes has to cancel the false routes originated from it to avoid being identified. In most of the 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 a pro-active protocol 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 by the real ones. 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 throughout the network. It is more difficult for the attacker in AODV to silently cancel the false routes.

V. Simulation Results

We study the practical impacts of the attacks on the performance of Ad Hoc networks through simulation. Two attacks on AODV are considered: false distance vector and false destination sequence. Except for sending false routes, the attacker will discard any data packets passing through it. We have designed two test conditions to examine their impacts. Under condition one, all connections have the same destination. We measure the delivery ratio, attack overhead, and the propagation of false routes when the malicious host attacks 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. We first describe the simulation environment and present the two cases separately.

A. Simulation Environment

The simulation of attacks on AODV is deployed using ns2 with CMU extension blocks for Ad Hoc networks [35]. Table I lists the simulation parameters.

TABLE I
Simulation Parameters.

Simulator	ns-2
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
Traffic type	CBR (UDP)
Data payload	512 bytes
Packet rate	2 pkt / s
Number of malicious host	1
Host pause time	10 seconds

The choice of the parameters considers 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 be too high and affect the performance degradation caused by attacks. The packet rate of connections is chosen to avoid packet drop caused by 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.

The first metric is selected to evaluate the percentage of packets that are affected by the attacks. This can be viewed as the ”strength” of an attack. The second metric is used to examine the overhead of different attacks. Here we consider only the extra cost on communication. If more comprehensive analysis is required, the overhead on computation and storage should be explored. The third metric examines the propagation of false routes and the potential impacts that are not included in the first metric. Together with metric two, we can collect a more comprehensive view of the impacts of the attacks.

B. Results of condition one

Under condition one, all connections have different sources and use node 29 as the destination. Node 5 is the malicious host and it attacks every RREQ that it receives. We observe selected parameters against the number of connections. Because there are 30 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 an average value of data collected from ten different host movement 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 scenarios: when node

5 does not conduct attacks, when it attacks the routes with false distance vector, and when it attacks the routes with false destination sequence. From figure 1 we note that the impact of the false destination sequence attack is more severe than that of false distance vector attack. The reason is that AODV prefers fresh routes to short ones.

One interesting observation is that when the network is under attack, the delivery ratio will increase slowly as the number of connections increases. This is due to the fact that the attacker does not apply any intelligent destination sequence prediction methods. On the contrary, the malicious host adds a constant to the sequence in RREQ and uses the result as the sequence in RREP. As the number of connections increases the true sequence increases faster. The probability that the chosen fake sequence is smaller than the true one also increases. Thus less traffic will be attracted to the attacker. From figure 1, we observe that one aggressive attacker may cause about 45% or 75% of the packets to be dropped. The impacts of active attacks on Ad Hoc networks are much more severe than those of passive attacks.

Figure 2 shows the number of hosts that are cheated by the false routes versus the number of connections. As the number of connections increases more false RREP will be sent by the attacker. Therefore more normal hosts will be cheated. From figure 2 we find that false destination sequence attacks can cheat up to 70% of the hosts in the system while the false distance vector attacks only cheat less than a half of the hosts. It is determined by the properties of the two attacks. A host will choose the false distance vector route only when it is closer to the attacker than to the real destination. If the hosts are uniformly distributed in the test area, it is not difficult to conclude that about half of the hosts will be closer to the attacker. They will be cheated if the sequence number in false routes is the same as in the real ones. Because AODV gives the destination sequence a higher priority, the false destination sequence attacks can cheat all hosts except the real destination. This explains the difference between the impacts of two attacks shown in figure 2. It also explains the difference between the delivery ratio curves shown in figure 1. When the network is under false distance vector attacks, about 50% of the packets reach their destination. But when the network is under false destination sequence attacks, the delivery ratio is much lower.

Figure 3 shows the communication overhead of the two attacks. Because in AODV every RREP can only attack one RREQ, the number of false RREP sent by the attacker is roughly proportional to the number of connections. The curves for the two kinds of attacks are very close to each other. It shows that both attacks put similar traffic overhead on the attacker. But the curve for false destination sequence attacks is a little higher. It is because the false destination sequence numbers sent by the malicious host disturb the updates of real number and introduce more route queries into the system.

Figure 4 examines the number of hosts got cheated versus the number of false RREP sent by the attacker. It can be viewed as the “efficiency” of the attacks. Combining data from figure 2 and figure 3, it is not difficult to explain the reason that figure 4 has similar observations as figure 2. Sending the same number of false RREP, attacks on destination sequence can cheat more hosts because AODV is in favor of fresh routes.

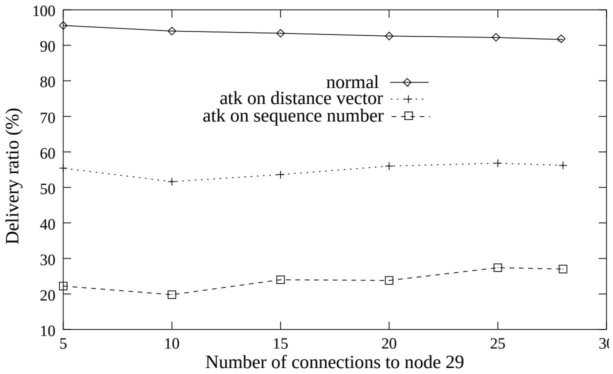

Fig. 1. The delivery ratio versus the number of connections to node 29.

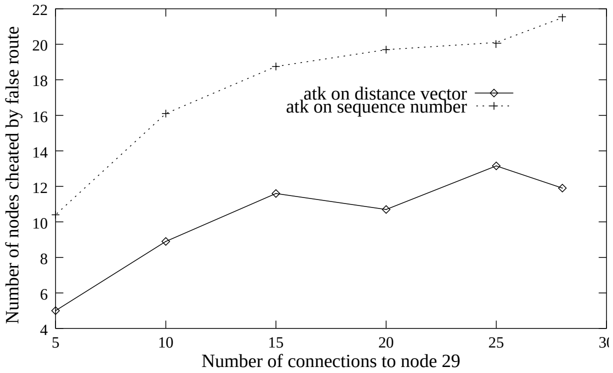

Fig. 2. The number of hosts got cheated versus the number of connections to node 29.

Combining the four figures, we note that the attacks on destination sequence and the attacks on distance vector have about the same overhead but the former has more severe impacts. For the intrusion prevention and intrusion detection systems designed to protect Ad Hoc networks using AODV, this kind of attack should be considered first.

C. *Results of condition two*

Under condition two, we generate a connection scenario in which each of the twenty-nine normal hosts is the source of one connection and the destination of another connection. Node 5 is the attacker. We study the selected parameters versus the mobility of the hosts, which is represented by the maximum moving speed. The results are shown in figure 5 and 6.

Figure 5 shows the delivery ratio versus the maximum speed of hosts under the scenarios the same as in figure 1. The delivery ratio under normal condition does not vary a lot. It shows that the mobility of host is still within the suit-

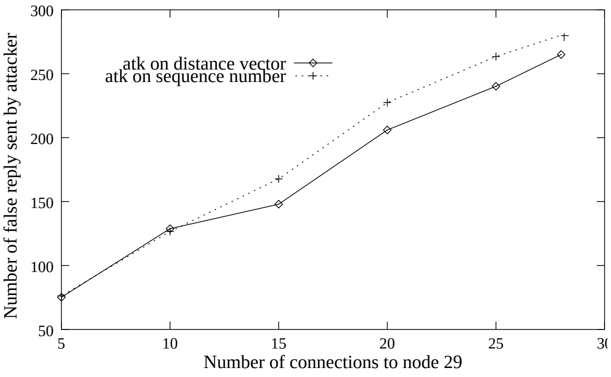

Fig. 3. The false RREP sent by attacker versus the number of connections to node 29.

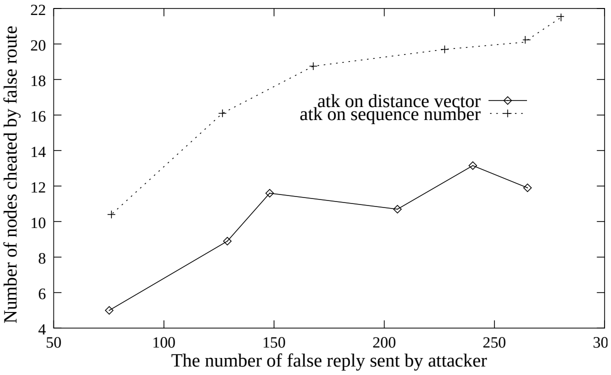

Fig. 4. The number of hosts got cheated versus the false RREP sent by attacker.

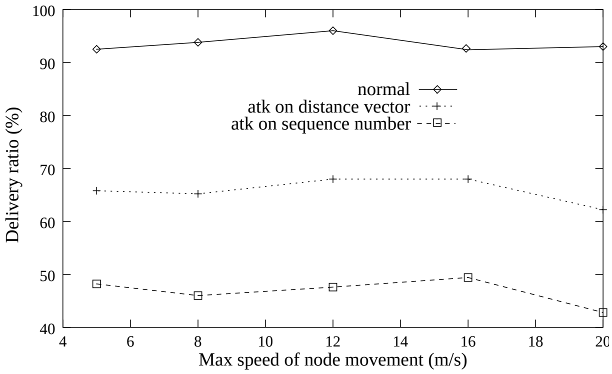

Fig. 5. The delivery ratio versus the mobility of hosts.

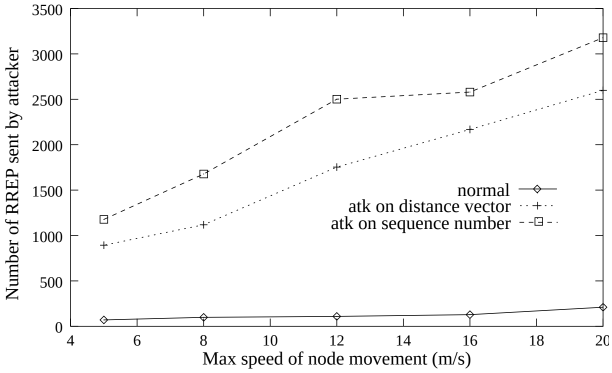

Fig. 6. The attack overhead versus the mobility of hosts.

able serving range of AODV. When the network is under attack, the delivery ratio only fluctuates within a small range. This is because the route changes caused by host movement put challenges on both the normal hosts and the attacker. The broken routes lead to the drop of packets. On the other hand, because of the break of false routes, the source hosts will activate the route discovery procedures and they have chance to construct the paths that do not pass through the malicious host. When the source hosts send out requests, other hosts can update their routing tables through the paths that they receive the RREQ. They take effects at the same time and keep the delivery ratio roughly stable. Compared to figure 1, we find that more data packets arrive at the destinations under attacks. 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. It will broadcast the RREQ throughout the network. Other hosts can establish the routes through the paths from which they receive the request. Therefore many hosts do not have to listen to the false RREP sent by the attacker. More true routes are set up and the delivery ratio is higher.

Figure 6 shows the number of RREP sent by node 5 when it behaves properly and when it conducts the attacks. Compared to the normal condition, the attacker will send five to ten times more RREP when it attacks every request that it receives. If the mobile hosts monitor the nearby traffic, this anomalous increase can be used as the pattern to activate IDS to examine possible attacks.

VI. Detecting False Destination Sequence Attacks on AODV

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 [36] tries to collect information and patterns of attacks and to provide the guidelines for the design of the intrusion detection systems. An example of detecting attacks on destination sequence in AODV is discussed next.

From the simulation results, we find that the attack on destination sequence has the worst impacts on data delivery ratio. To “beat” other available routes, the attacker must choose a large number as the false sequence to show its “freshness”. The false number will be larger than the sequence generated by the real destination. Later 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

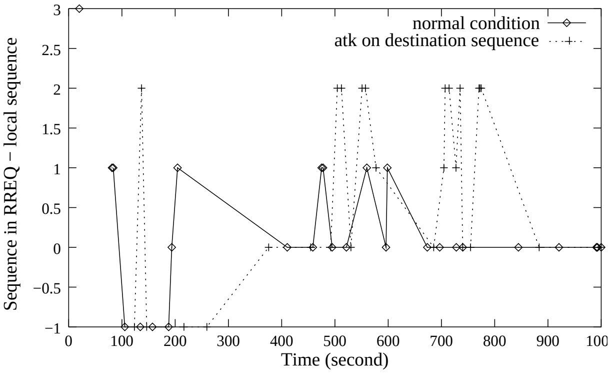

Fig. 7. The difference between two sequences when the network is normal and when the host is under destination sequence attack.

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 number is still larger than the real sequence, the destination host will find that it is under attack. The detection of false destination sequence attacks in AODV heavily depends on the mobility of hosts. Therefore, no upper limit of delay between the attack is conducted and it is detected can be guaranteed.

Under normal operation of AODV, the destination sequence number carried in RREQ can never be larger than the real sequence plus one. But when a host is under attack on destination sequence, the difference between the received and local sequence numbers will be equal or larger than 2. Figure 7 gives an example of the difference between the two sequence numbers detected by a normal host. When it is under attack, the normal host detects eleven times that the incoming sequence number is larger than local number plus one in one thousand seconds of simulation time.

From the analysis we know that some false sequence numbers are not detected. Two problems that impact the detection of false destination sequence attacks in AODV are: (1) The real sequence may outrun the false one when it is received by the victim. Then the host cannot find the false number. (2) A tighter limit of the delay between the false sequence is generated and it reaches the victim, if the two hosts are connected, should be achieved. We are working on the solutions to these problems. A protocol that uses one detected attack to activate the detection of other attacks has been designed in AODV [33]. The basic idea is to re-examine all routing information coming from the same sources and activate the re-discovery.

Collecting and determining the anomaly patterns of attacks is a challenging topic in intrusion detection in Ad Hoc networks and is still under research. The example provided above shows that by combining the protocol analysis and practical simulation we may accelerate this procedure. We plan to apply this mechanism to the establishment of our IDS and the design of a secure routing protocol.

VII. 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 and attacks on one of the protocols – AODV. The analysis shows that although AODV provides fair performance with reasonable overhead and provides adaptability to both traffic load and host mobility, the on-demand property allows the malicious host to attack the network in real time with flexibility. It is difficult to locate the sources of the false information. The attacks may lead to the confusion on network connectivity or exhaustion of the limited bandwidth, thus degrading the performance of the networks. The simulation has shown that the attacks can drastically lower the delivery ratio and cheat a considerable part of the hosts with false routes.

The research on protecting wired network routing protocols [37] has shown that it is the property, instead of the protocol detail, that leads to the vulnerability. The example attacks on AODV (false distance vector, false destination sequence) can also be applied to attack other protocols sharing the properties (e.g. DSDV). Thus the theoretical analysis of the vulnerability and anomaly patterns of the attacks can be employed to prevent or detect the conterminous attacks on different protocols. The paper presents the detection of false destination sequence attacks by monitoring the sequence numbers carried in RREQ. This detection method can be applied to protect DSDV with minor changes.

There are many problems to be solved in protecting the Ad Hoc networks. We plan to study other features of the routing protocols to exploit their security vulnerabilities. The robustness comparison among the routing protocols (such as AODV, DSDV, and ZRP) against conterminous attacks (e.g. false distance vector) will be conducted. On achieving the secure distribution of individual intrusion detection results, we plan to establish the trust relation among hosts in the open area of Ad Hoc networks [38]. The results will provide the guidelines for the design of a secure Ad Hoc routing protocol and form the building blocks of an IDS for Ad Hoc networks.

REFERENCES

[1] M. Corson and A. Ephremides, "A distributed routing algorithm for mobile radio networks," in *Proceedings of Military Communications Conference*, 1989.

[2] R. Ramanujan and R. Edin, "TIARA: Techniques for intrusion-resistant Ad Hoc routing algorithms," DARPA funded proposal, www.oracorp.com/projects/current/tiara.html, 2000-2003.

[3] 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.

[4] D. Johnson and D. Maltz, *Dynamic Source Routing in Ad Hoc Wireless Networks*, Kluwer Academic Publisher, 1996.

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

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

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

[8] S. Murthy and J. Aceves, "An efficient routing protocol for wireless networks," *Mobile Networks and Applications*, vol. 1, no. 2, pp. 183–197, 1996.

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

[10] T. Camp, J. Boleng, B. Williams, L. Wilcox, and W. Navidi, "Performance comparison of two location based routing protocols for Ad Hoc networks," in *Proceedings of the IEEE INFOCOM*, 2002.

[11] Z. Haas, J. Halpern, and L. Li, "Gossip-based Ad Hoc routing," in *Proceedings of the IEEE INFOCOM*, 2002.

[12] C. Perkins, E. Royer, and S. Das, "Performance comparison of two on-demand routing protocols for Ad Hoc networks," in *Proceedings of IEEE INFOCOM*, 2000.

[13] S. Das and R. Sengupta, "Comparative performance evaluation of routing protocol for mobile, Ad Hoc networks," in *Proceedings of IEEE the Seventh International Conference on Computer Communications and Networks*, 1998.

[14] L. Venkatraman and D. Agrawal, "Authentication in Ad Hoc networks," in *Proceedings of the 2nd IEEE Wireless Communications and Networking Conference*, 2000.

[15] P. Nikander, "Authentication, authorization, and accounting in Ad Hoc networks," in *Proceedings of the Helsinki University of Technology Seminar on Internetworking*, 2000.

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

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

[18] Z. Zhou and Z. Haas, "Secure Ad Hoc networks," *IEEE Networks*, vol. 13, no. 6, pp. 24–30, 1999.

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

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

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

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

[23] S. Bhargava and D. Agrawal, "Security enhancements in AODV protocol for wireless Ad Hoc networks," in *Proceedings of Vehicular Technology Conference*, 2001.

[24] 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.

[25] 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.

[26] Z. Haas, "Secure communication for Ad Hoc networking," NSF funded proposal, http://wnl.ece.cornell.edu/wnlprojects.html, 2000-2003.

[27] D. Agrawal, "On robust and secure mobile Ad Hoc and sensor netwroks," NSF funded proposal, http://www.ececs.uc.edu/ cdmc/, 2001-2004.

[28] Wenke Lee, "CAREER: Adaptive intrusion detection systems," NSF funded proposal, http://www.cc.gatech.edu/ wenke/, 2002-2005.

[29] E. Royer and C. Perkins, "Multicast operation of the Ad Hoc on-demand distance vector routing protocol," in *Proceedings of MobiCOM*, 1999.

[30] M. Marina and S. Das, "On-demand multipath distance vector routing in Ad Hoc networks," in *Proceedings of IEEE International Conference on Network Protocols (ICNP)*, 2001.

[31] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, 1999.

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

[33] W. Wang and B. Bhargava, "On vulnerability and protection of AODV," Technical report, TR-2002-18, CERIAS Security Research Center, Purdue University, http://raidlab.cs.purdue.edu, 2002.

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

[35] "http://www.isi.edu/nsnam/ns/," Sep. 2002.

[36] B. Bhargava, "Trusted routing and intruder identification in mobile Ad Hoc networks," CERIAS funded proposal, 2002-2003.

[37] S. Bellovin, "Security problems in the TCP/IP protocol suite," *Computer Communications Review*, vol. 19, no. 2, pp. 32–48, April 1989.

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