INCREASING THE DOS ATTACK RESILIENCY IN MILITARY AD HOC NETWORKS[1]

Jarmo V. E. Mölsä
Communications Laboratory, Helsinki University of Technology
P.O. Box 3000, FI-02015 HUT, Finland

ABSTRACT

This paper investigates resiliency of three ad hoc routing protocols against the range attack. This Denial of Service (DoS) attack has not been described in the literature before. It is based on modifying the transmission range of a wireless node periodically which causes continuous changes in the topology of an ad hoc network. The range attack does not require a node to be compromised. An enemy only has to get close enough to a node to attenuate or amplify radio signal. The research methodology is based on using the ns-2 network simulator to analyze the transmission delay in a small ad hoc network. An enemy uses one of the nodes to carry out the range attack. The following ad hoc routing protocols were compared: the Destination-Sequenced Distance-Vector (DSDV), the Ad hoc On-demand Distance-Vector (AODV), and the Dynamic Source Routing (DSR) protocols. According to the simulation results, DSDV provides the best resiliency against the range attack when the primary application requires a very short transmission delay less or equal to 0.1 seconds. When the primary application tolerates delays up to 2 seconds, AODV provides the best resiliency against the range attack. Defense mechanisms are thus situation dependent. A control system is required to change defense mechanisms, if application requirements change.

INTRODUCTION

Denial of Service (DoS) attacks are a more serious threat in mobile ad hoc networks than in wired networks due to the complexity, resource constraints, dynamic network topology, open network architecture, and shared transmission media [13]. The higher the complexity of a system, the more possibilities there are to be exploited for attack purposes. Resource constraints restrict the ability to handle and withstand attacks due to limited processing power, transmission bandwidth, and lifetime of batteries. Dynamic network topology places a burden on routing protocols when trying to achieve short reaction and convergence times. Open network architecture and shared transmission media make it possible to join a network without a physical connection. Any of these vulnerabilities can be exploited in a DoS attack to prevent or delay legitimate access to services.

This paper studies the *range attack*, which is a new DoS attack not described in the literature before. In the range attack the transmission range of a wireless node is periodically modified to cause a varying network topology. An attacker does not have to compromise a wireless node to carry out a range attack. Instead an attacker only needs to get close to a node to attenuate or amplify the radio signal. The routing protocol is responsible for adapting to a change in topology. For this reason, ad hoc routing protocols should be seen as defense mechanisms against the range attack.

The primary contribution of this paper is to investigate resiliency of three ad hoc routing protocols against the range attack. The routing protocols are the Destination-Sequenced Distance-Vector (DSDV), the Ad hoc On-demand Distance-Vector (AODV), and the Dynamic Source Routing (DSR) protocols. The research methodology is based on using the ns-2 network simulator for analyzing the transmission delay in a small ad hoc network. One node of this ad hoc network is used by an enemy to carry out the range attack.

It is argued in this paper that effectiveness of DoS defense mechanisms is situation dependent, i.e. different defense mechanisms are useful for different applications. The simulation results indicate that DSDV provides the highest resiliency against the range attack when applications require a very short transmission delay less or equal to 0.1 seconds. When applications tolerate a longer delay up to 2 seconds, AODV was found to provide the highest resiliency against the range attack.

AN OVERVIEW TO AD HOC ROUTING PROTOCOLS

This paper compares resiliency of DSDV, AODV, and DSR protocols against the range attack. These three ad hoc routing protocols are described shortly here.

DSDV [7] is a proactive, table-driven routing protocol. Every node maintains a routing table which contains an entry for all destination nodes in an ad hoc network. Each node periodically broadcasts the contents of its routing table. Substantial route changes can be advertised separately as triggered updates. Fluctuations in routes are

[1] This work was funded by the Finnish Defence Forces.

dampened by delaying a triggered update by a specific length of time called the settling time. The settling time should be long enough so that the best route advertisement is received within this time. The amount of control traffic in DSDV is independent of the application data transmitted in the network. Even if there is no application data to be transmitted, DSDV will still update routes to all destinations at all nodes. There is no possibility for a node to request a route to a destination, but instead a node must wait until some neighbor decides to advertise a route to the destination. Especially during startup it will take some time until routes are propagated through the whole network. The larger the diameter of an ad hoc network as hops, the longer the convergence time. In the ns-2 network simulator periodical broadcasts (containing the whole routing table of a node) are transmitted randomly every 11.25 – 15 seconds, and the settling time is initially 12 seconds.

AODV [6] is a reactive, on-demand routing protocol. Each node maintains routes only for those destinations to which data is actually sent. A route is removed from the routing tables after the route is no longer used. Route discovery begins when a source node has some data to be sent to a destination for which there is no route available in the local route table. In this case the source node broadcasts a route discovery (RREQ) message. A node receiving RREQ message will rebroadcast the message. Finally the destination node will respond to the request with a unicast route response (RREP) message, provided that the ad hoc network is not partitioned. An intermediate node may also respond with an RREP message if it knows the requested route. RREQ and RREP messages set up a routing table entry for the destination in all nodes on the path. If the route is broken after a topology change, a route error (RERR) message is returned to the originating node as a response to a data message, and a new route discovery is initiated before resending of the data message is possible. In the ns-2 network simulator the maximum lifetime for an unused route table entry is 10 seconds. If no data is transmitted to a destination within this time, the corresponding route table entry is expired.

DSR [5] is a reactive, on-demand routing protocol. The source node sending a data message will decide the route the message will traverse. The route is stored as a source route in the message header. Intervening nodes on the path will forward the message according to this source route. Route discovery and route maintenance are similar to AODV. When a source node has data to be sent to a destination, the source node broadcasts a ROUTE REQUEST message. All intervening nodes store their address in the header of the ROUTE REQUEST message as it is forwarded. The destination will finally respond with a ROUTE REPLY message including the route from the ROUTE REQUEST message. If a source route is broken after a topology change, a ROUTE ERROR message is returned to the originating node. The control traffic overhead is small, as there is no control traffic when no data is being sent. Created routes do not have a lifetime, so routes are not expired. In the ns-2 network simulator the promiscuous receive mode is enabled by default, and nodes can store information about all routes they can hear, even from messages for which they are not a recipient. An intermediate node is allowed to reply to a request using cached routes. Also, the ns-2 implements by default a two-stage route discovery process. First a source node sends a non-propagating request to try to find out whether the destination is a direct neighbor. If a reply is not received soon, a propagating request message is sent.

STRUCTURE OF THE SIMULATED NETWORK

The ns-2.28 network simulator was used to study the resiliency of different ad hoc routing protocols against the range attack. The following two modifications were made to the ns-2.28 network simulator: nodes were allowed to have different transmission ranges, and the DSDV infinite loop problem was patched. The structure of the simulated network is shown in the Fig. 1.

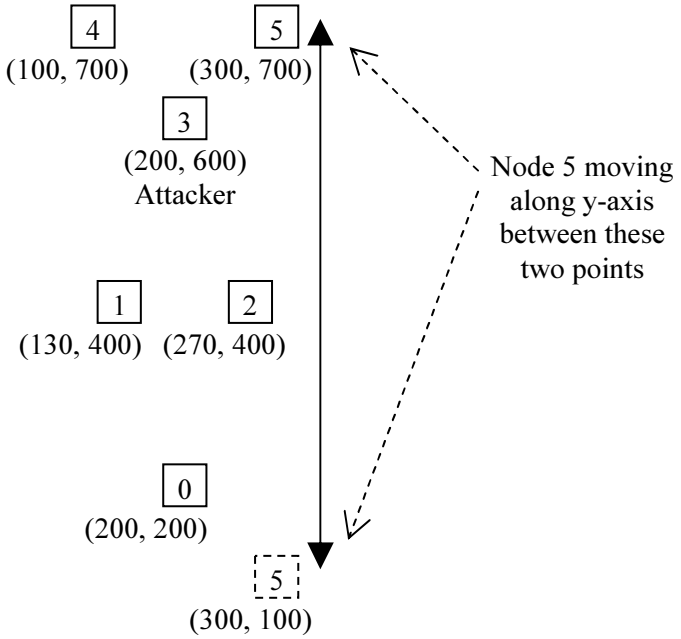

Figure 1. The structure of the simulated ad hoc network. The node 3 is used for the range attack.

The simulated ad hoc network consists of six nodes, numbered from 0 to 5. The x- and y-coordinates of the nodes are shown in parenthesis below the node. Nodes 0 to 4 are static. The node 5 is moving along the y-axis, and its initial point is (300, 700). At the beginning of a simulation the node 5 starts moving towards point (300, 100) at the speed of 3 m/s. At the time of 400 seconds the node 5 starts moving backwards to point (300, 700). The node 5 initiates a movement every 400 seconds.

The node 3 is used for the range attack. If the *range attack length* is *x* seconds, the transmission range of the attacker's node changes every *x* seconds: first the transmission range has the default value of 250 meters, then the range is attenuated to 40 meters, and then range is restored to 250 meters, and so on. The transmission range is constant for every period of *x* seconds.

All five client nodes are automatically downloading web pages from the server node 0 over the Transmission Control Protocol (TCP). Each web page is 2920 bytes in length, which results in two full-size TCP segments. Maximum Segment Size (MSS) for TCP is here thus 1460 bytes. It is expected that persistent TCP connections are used. Each download transaction consists of the transmission of the two TCP segments (required here by one web page) from the node 0. The download transaction is finished when the TCP acknowledgements for both of the TCP segments are received by the node 0. The *transmission delay* of a single web page is thus the time from the transmission of the first TCP segment until the acknowledgement for the second TCP segment has been received at the node 0. After the transaction, the connection is completely ready for the next download. Web pages are downloaded with an exponentially distributed inter-page time. The average inter-page time for all legitimate clients was 30 seconds. Attacker's average inter-page time was varied within the range of 1-30 seconds to see how additional attack traffic changes the results. Modifying the attacker's inter-page time requires that the attacker has access to applications running in the node.

All nodes are using the 802.11 Medium Access Control (MAC) with Distributed Coordinated Function (DCF). All unicast messages are preceded with a Request-To-Send (RTS) and a Clear-To-Send (CTS) control messages, and all unicast messages are acknowledged at the MAC level. All broadcast messages are transmitted without any MAC level message overhead. All messages are transmitted with the bandwidth of 1 Mbps.

SIMULATION PARAMETERS

The length of one simulation was 60 000 seconds. Due to the memory requirements of DSR, every simulation was divided into 15 independent sub-simulations, each of length 4 000 seconds. Each of these independent sub-simulations was using different random number sequences. Simulations were repeated with all the following parameter combinations:

- Attacker's average inter-page time was 1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, 5, 5.5, 6, 6.5, 7, 8, 9, 10, 12, 15, 17, 20, 22, 25, 27, or 30 seconds.
- The range attack length was 1, 2, 5, 10, 15, 20, 25, or 30 seconds.
- The routing protocol was DSDV, AODV, or DSR.

In all the following figures the transmission delays to all legitimate nodes 1, 2, 4, and 5 are combined and shown as a single curve. All graphs have three different curves, one for each ad hoc routing protocol.

SIMULATION RESULTS FOR THE DISTRIBUTION OF THE TRANSMISSION DELAY

The Fig. 2 shows the Cumulative Distribution Function (CDF) for the delay to all legitimate client nodes when there is no range attack. Figures 3 and 4 show the CDF for the transmission delay when the range attack length is 30 seconds and 1 second, respectively.

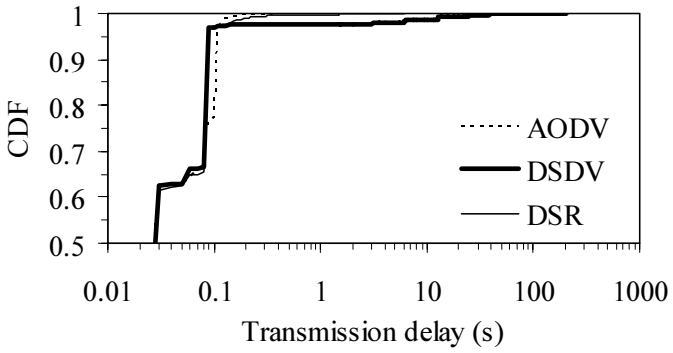

Figure 2. CDF for delay. No range attack.

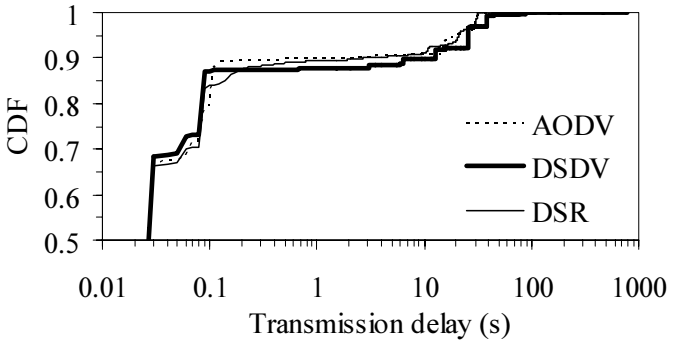

Figure 3. CDF for delay. Range attack length is 30 s.

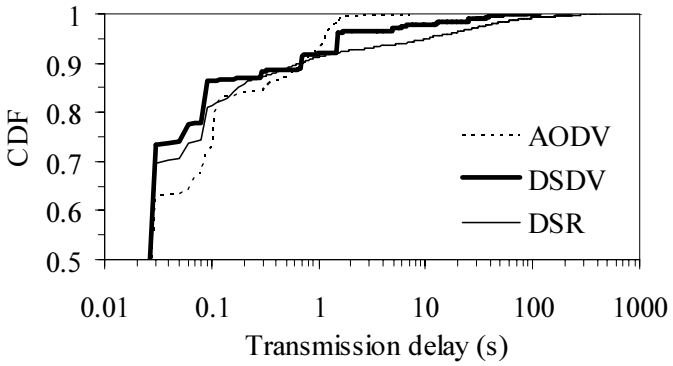

Figure 4. CDF for delay. Range attack length is 1 s.

The x-axis of figures 2, 3, and 4 shows the transmission delay as seconds on a logarithmic scale. The y-axis shows the CDF. CDF(X) is the probability that the transmission delay is less or equal to X. The average inter-page time for the node 3 is 30 seconds in all of these three figures.

Figures 3 and 4 indicate that the resulting CDF depends on the attack characteristics. DSDV is the most resilient routing protocol against the range attack, when short transmission delays are required by the primary application in an ad hoc network. AODV provides the best overall resiliency against the range attack when longer delays are tolerated. DSR cannot provide a consistently good resiliency against the range attack.

When comparing figures 3 and 4 to figure 2 we can see that approximately 10 % of the web page transmissions suffer from the range attack. The transmission delay for this 10 % of web pages is at least 10 or 100 times the delay without an attack. All of the deterioration in the transmission delay affects only nodes 4 and 5, which are dependent on multi-hop connections through the attacker's node. Nodes 1 and 2 have a direct connection to the node 0.

In Fig. 3 all CDF curves are relatively flat on the range from 0.2 to 10 seconds. In Fig. 4 all CDF curves are relatively flat on the range from 0.2 to 1 second. The length of the flat interval depends on the length of the range attack. When the transmission range is small it is not possible to have multi-hop connections through the node 3. This forces TCP to wait until the longer transmission range reenables an end-to-end connection. The longer the range attack length, the longer the flat interval of a CDF curve. Despite of the long simulation times all CDF curves have clear steps. This is mostly due to TCP-timeouts. After a timeout, TCP doubles the next timeout length.

SIMULATION RESULTS FOR AN APPLICATION REQUIRING SHORT DELAYS

This section describes how resilient the three ad hoc routing protocols are against the range attack when the network is used to transfer information with a very strict delay requirement. It is expected here that the information must be transmitted within 0.1 seconds to an automated application requiring no human intervention. If the transmission delay is longer than 0.1 seconds, the information gets useless due to becoming old. An example of this kind of an application can be the air defense.

Figures 5, 6, 7, and 8 indicate the fraction of transmissions having a delay less or equal to 0.1 seconds. In figures 5 and 6 this fraction is shown as a function of the range attack length, when the attacker's inter-page time is 30 s and 5 s, respectively. In figures 7 and 8 the fractions are shown as a function of the attacker's inter-page time, when the range attack length is 30 s and 1 s, respectively.

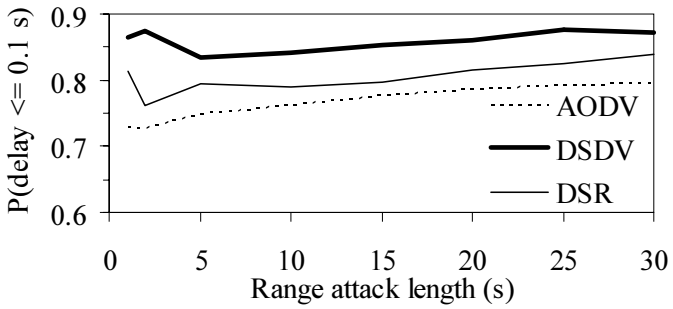

Figure 5. Fraction of transmissions having a delay less or equal to 0.1 s. Attacker's inter-page time is 30 s.

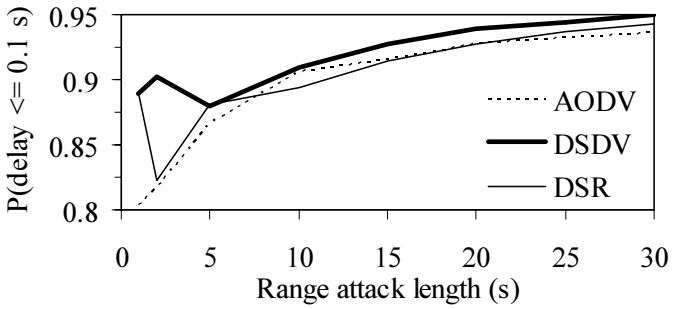

Figure 6. Fraction of transmissions having a delay less or equal to 0.1 s. Attacker's inter-page time is 5 s.

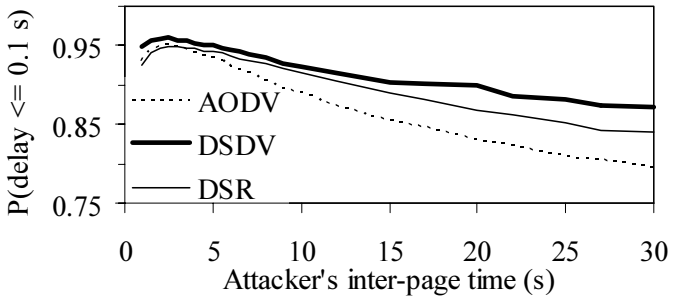

Figure 7. Fraction of transmissions having a delay less or equal to 0.1 s. Length of the range attack is 30 s.

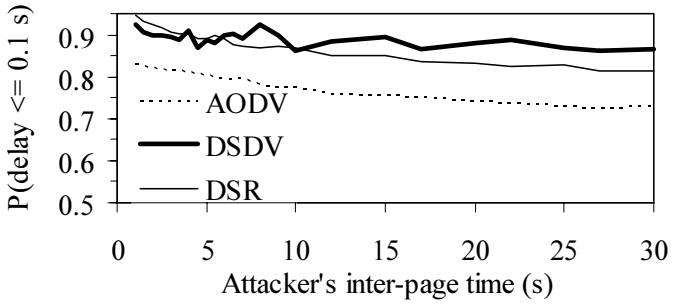

Figure 8. Fraction of transmissions having a delay less or equal to 0.1 s. Length of the range attack is 1 s.

As can be seen from the above figures, DSDV provides the best resiliency against the range attack when short transmission delay is required. Here, AODV provides the worst

overall resiliency against the range attack. One reason for the good performance of DSDV here is that it is proactive and a high proportion of web-page downloads does not have to wait for a route setup.

SIMULATION RESULTS FOR AN APPLICATION TOLERATING RELATIVELY LONG DELAYS

This section describes how resilient the three ad hoc routing protocols are against the range attack when the network is used to transfer information for humans with a flexible delay requirement. The maximum transmission delay allowed is here 2 seconds. An example of an application with this kind of a delay requirement is a situational awareness application providing information for humans. Figures 9, 10, 11, and 12 indicate the fraction of transmissions having a delay less or equal to 2 s.

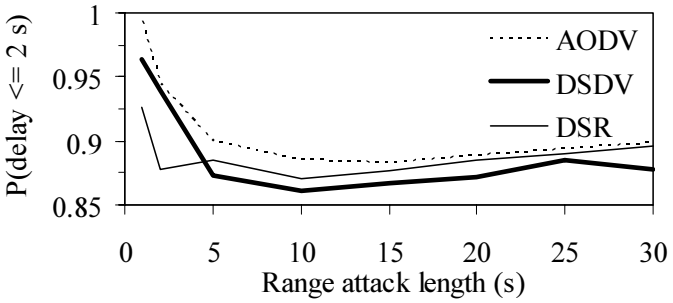

Figure 9. Fraction of transmissions having a delay less or equal to 2 s. Attacker's inter-page time is 30 s.

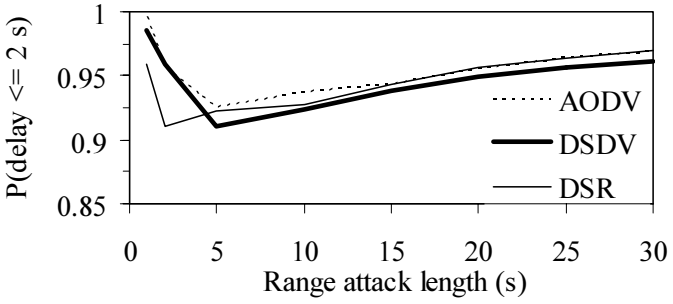

Figure 10. Fraction of transmissions having a delay less or equal to 2 s. Attacker's inter-page time is 5 s.

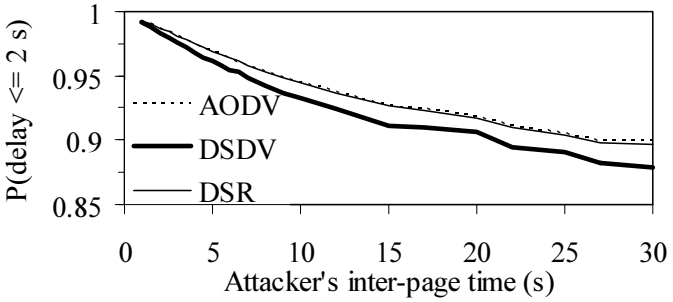

Figure 11. Fraction of transmissions having a delay less or equal to 2 s. Length of the range attack is 30 s.

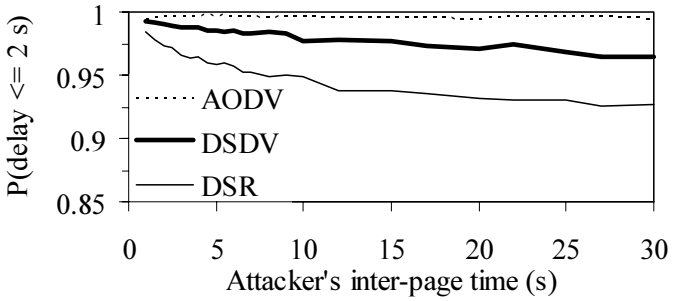

Figure 12. Fraction of transmissions having a delay less or equal to 2 s. Length of the range attack is 1 s.

According to these results, AODV is the most resilient protocol against the range attack when applications allow a relatively long transmission delay. AODV is better than DSDV in all these four figures. One reason for the good performance of AODV here is that it is faster in finding a new route than DSDV. With DSDV the delay for setting up a new route after a topology change is at least approximately 12 seconds in ns-2. The performance of DSR varies. Sometimes it provides as good resiliency as AODV. In the Fig. 12, however, DSR lags clearly behind of both AODV and DSDV.

Generally, the fraction of transmissions fulfilling the delay requirement increases as the function of the range attack length, as can be seen clearly in figures 5, 6, and 10. The reason for this seems to be the synchronization of the sources with the range attack frequency. Sources will synchronize better when the range attack length has a similar length as the average inter-page time. A web page download is omitted if the previous download is not yet finished, and a new download time is chosen.

In the Fig. 10 both the DSDV and the AODV curves have the lowest performance when the range attack length is 5 s. The fraction of transmissions fulfilling the delay requirement is high when the range attack length is 1 or 2 seconds, because applications can tolerate up to one complete period of range attack and still achieve the delay requirement. Also, short topology changes may not even be noticed by a routing protocol. Thus, to make an effective attack, the range attack length should not be too short and not too long.

Surprisingly, the curves in figures 7, 8, 11, and 12 are mostly decreasing, which means that ad hoc routing protocols perform better when there is more attack traffic. If a network is lightly loaded, additional traffic makes it faster to notice topology changes, and prevents correct routes to be expired. If complete flooding is not the goal for an attacker (e.g., to make an attack more difficult to detect), the amount of additional traffic in lightly loaded networks should be minimized to make a range attack more effective.

INCREASING THE RESILIENCY AGAINST DOS ATTACKS

The previous results indicate that effectiveness of DoS defense mechanisms is situation dependent. If an ad hoc network is used by an application requiring a very short transmission delay (less or equal to 0.1 seconds), DSDV provides the highest resiliency against the range attack and AODV the lowest resiliency. This result turns upside down when the ad hoc network is used by an application accepting a longer transmission delay (less or equal to 2 seconds). In this case AODV provides the highest resiliency against the range attack. The resiliency of ad hoc routing protocols against the range attack depends thus on the requirements of the primary application used in an ad hoc network.

In general, the characteristics of applications should be considered when evaluating and choosing defense mechanisms against DoS attacks. The following list gives some characteristics important in this process:

- Transmission delay: Does the primary application used in the network have a strict delay requirement, i.e., how dependent an application is on a short transmission delay? What is the maximum delay accepted?
- Variability in transmission delay: How much jitter in delay is tolerated?
- Throughput: How much throughput is required for minimum, decent, or good application performance?
- Variability in throughput: How dependent applications are on even throughput?
- Transmission breaks: How does an application react on transmission breaks? What is the maximum length of a transmission break still tolerated by an application?
- Reliability of data transfer: Should all data be transmitted reliably, or can some intervening data be lost? A TCP connection waiting for acknowledgements may have to be finished, because a connection may stay in a wait state for quite a long time.
- Connection initiation delay. If connections are shutdown and rebuilt for every purpose, how fast should a new connection be created?
- Reaction to network service degradation: If network service degrades heavily, should a connection be rather terminated than continued in a low-quality mode?
- Adaptation capabilities: Is an application able to adapt to varying quality of network service, for example, by being able to use compression algorithms of different strength? Is it possible to aggregate data or otherwise decrease the frequency transmissions?
- Application structure: Is an end-to-end connection always required, or is it possible to use intermediate nodes as proxies or caches for nodes with intermittent connectivity? In other words, is it possible to move important data closer to destinations for which an end-to-end connection is not available?

The selection of defense mechanisms against DoS attacks requires first the assessment of application requirements, for example, according to the characteristics in the list above. When the requirements of the primary applications are known, then the properties of available defense mechanisms can be evaluated. The defense mechanisms providing the best match with the requirements should be selected.

Especially in military networks the requirements of applications and even the primary application may change as a function of time. For example, applications used during a tactical attack may have completely different requirements than those applications used during a non-attack time. For this reason, military networks should be able to change the defense mechanisms according to the primary application. A control system is thus required to change the defense mechanisms to suit the requirements of applications. The following list gives some requirements for a control system:

- If a defense mechanism is used by all individual nodes (like the routing protocol in ad hoc networks), all nodes should start using the new defense mechanism approximately at the same time.
- As an ad hoc network can be partitioned, the control system should be able initiate the change of a defense mechanism at a pre-specified time in the future. All nodes should receive this message in time.
- The reception of a control message to change a defense mechanism should by acknowledged system-wide. Depending on the defense mechanism it may not be feasible to start using a defense mechanism in only a subset of the nodes. All nodes should know if all nodes are able to change the defense mechanism.

Any defense mechanism should be stable enough so that too frequent changes can be avoided. If a defense mechanism fits only a very narrow class of application requirements, a change is needed more often than with defense mechanisms fitting a broader class of requirements.

RELATED WORK

The misuse of routing protocols seems to be the most widely studied subtype of DoS attacks in ad hoc networks, for example in [3], [11], and [13]. Fewer papers study other types of DoS attacks in ad hoc networks. For example, [12] describes many possible DoS attacks on different protocol layers in sensor networks, but most of it is applicable to ad hoc networks, too. The jelly fish attack described in [1] forces TCP flows to have almost zero throughput by simply reordering, dropping, or causing variable delay to TCP packets.

The performance of ad hoc routing protocols has been studied, for example, in [2] and [10]. In [9] the effect of mobility on ad hoc routing protocol performance was studied. DSDV provided the lowest route acquisition time, packet-delay, and control-packet overhead. AODV provided the best throughput.

The impact of the traffic pattern [8] and the mobility model [4] is significant on the performance of ad hoc routing protocols. Not only should the application requirements for the network performance be analyzed, but also the traffic pattern and mobility model in general.

CONCLUSIONS

This paper reported simulation results about how resilient different ad hoc routing protocols are against the range attack described in this paper. In the range attack an enemy periodically attenuates the strength of transmitted radio signal of a wireless node. This causes periodical topology changes which an ad hoc routing protocol must process for being able to send data to recipients.

The simulation results indicate that the selection of a defense mechanism is situation dependent. If an ad hoc network is primarily used by an application requiring a transmission delay less or equal to 0.1 seconds, DSDV provided the best and AODV the lowest resiliency against the range attack. If the primary application tolerated a longer transmission delay less or equal to 2 seconds, however, AODV provided the best resiliency against the range attack. The different requirement for the transmission delay turned effectiveness of the ad hoc routing protocols upside down.

According to the results, it is not possible to provide decent resiliency against the range attack with only a single defense mechanism independently of the type of application. It must be possible to change a defense mechanism when the application requirements change. A control system is required for this purpose.

ACKNOWLEDGEMENTS

The author would like to thank Jorma Jormakka for his helpful comments in improving this paper.

REFERENCES

[1] I. Aad, J.-P. Hubaux, and E. W. Knightly, "Denial of service resilience in ad hoc networks," in *Proceedings of the MobiCom*, Philadelphia, Pennsylvania, USA, Sep. 2004.

[2] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva, "A performance comparison of multi-hop wireless ad hoc network routing protocols," in *Proceedings of the MobiCom*, Dallas, Texas, USA, Oct. 1998.

[3] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," in *Proceedings of the WiSe 2003*, San Diego, California, USA, Sep. 2003.

[4] A. P. Jardosh, E. M. Belding-Royer, K. C. Almeroth, and S. Suri, "Real-world environment models for mobile network evaluation," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 3, pp. 622-632, Mar. 2005.

[5] D. B. Johnson, D. A. Maltz, and Y.-C. Hu. *The Dynamic Source Routing protocol for mobile ad hoc networks (DSR).* Internet draft, draft-ietf-manet-dsr-10.txt, Jul. 2004, work in progress.

[6] C. Perkins, E. Belding-Royer, and S. Das. *Ad Hoc On-Demand Distance-Vector (AODV) routing*. Internet Engineering Task Force, Request for Comments RFC 3561, Jul. 2003.

[7] C. E. Perkins, and P. Bhagwat, "Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers," in *Proceedings of the SIGCOMM '94 Conference on Communications Architectures, Protocols and Applications,* pp. 234-244, Aug. 1994.

[8] H. Pucha, S. M. Das, and Y. C. Hu, "The performance impact of traffic patterns on routing protocols in mobile ad hoc networks," in *Proceedings of the MsWiM*, Venice, Italy, Oct. 2004.

[9] S. Sesay, Z. Yang, B. Qi, and J. He, "Simulation comparison of four wireless ad hoc routing protocols," in *Information Technology Journal*, vol. 3, no. 3, pp. 219-226, 2004.

[10] C. Stavroulopoulos, T. Antonakopoulos, and V. Makios, "Performance evaluation of mobile ad hoc network routing protocols for real time applications support," in *Proceedings of COMCON '8,* Crete, Greece, Jun. 2001.

[11] W. Wang, Y. Lu, and B. K. Bhargava, "On security study of two distance vector routing protocols for mobile ad hoc networks," in *Proceedings of the IEEE PerCom,* Fort Worth, Texas, USA, Mar. 2003.

[12] A. D. Wood, and J. A. Stankovic, "Denial of service in sensor networks," IEEE Computer, vol. 35, no. 10, pp. 54-62, Oct. 2002.

[13] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: Challenges and solutions," *IEEE Wireless Communications,* vol. 11, no. 1, pp. 38-47, Feb. 2004.