Abstract—The general nature of ad hoc routing lends itself to be insecure since all the nodes in the network must rely on their peers for success. The existing DARS routing simulator currently only takes into account a perfect routing simulation environment. All the nodes in the network work cooperatively and there are no malicious nodes to cause degradation to the network infrastructure. This project aims to add those elements of security vulnerabilities to paint a better picture of what ad hoc networks face in a real world environment. The second goal of this project is to add gaming concepts to the simulator to provide a learning experience for computer science students.

Index Terms—Security, ad hoc, simulator, game, education, aodv, dsdv.

I. INTRODUCTION

THE lack of a completed open source ad hoc routing simulator led to the development of the DARS in 2010. The initial work on DARS strived to provide an ad hoc routing simulator that could be used for education and experimentation. Since the initial creation and release of DARS, little development has been done to the software. The goal of this effort is to expand on the initial work on DARS and add more features that can be used in the educational sector. The main area of focus for this project is to add security-related features to the already existing protocols. These features include various types of network attacks that can be used to disrupt the normal operation of the existing network protocols of AODV and DSDV. These malicious adaptations to the routing protocols can be used to demonstrate the unique difficulties of ad hoc networks. Each type of attack will be showcased in pre-canned scenarios that students will be able to play back and interact with at any time. This will allow a quick demonstration of how the attacks can be utilized. Challenges will also be added to the simulator to add a game-like feature to the simulator for students to participate. Beyond the direct goals of software modification lies the effort to provide a means of enabling educators and students with a mechanism to demonstrate the importance of security considerations for ad hoc networks and protocols.

II. BACKGROUND

A. Mobile Ad Hoc Routing Protocols

Mobile ad hoc Networks (MANETs) are wireless networks with little to no supporting infrastructure, such as routers. These networks pose difficult problems attempting to address mobile components to provide a connected network to as many users as possible. This is accomplished by passing packets from node to node within the network. Routing paths in these networks are normally discovered, or learned, from a series of broadcasting and receiving packets. Multiple protocols that are designed to function in this manner have been developed. Unlike standard routing protocols that can assume that routes are less volatile, these protocols must accept the fact that the nodes in the network are mobile and routes will change frequently.

B. Types of Protocols

Evaluating MANET protocols generally divides them into two types of protocols: Reactive and Proactive. Both types of protocols have distinct advantages and disadvantages which will be discussed in the following sections. There is a third type of protocol called a Hybrid protocol which uses concepts from both the reactive and proactive styles. DARS however, does not implement a hybrid protocol at this time so it will not be a focus for this paper.

1) Reactive: Reactive protocols such as AODV wait until something of importance is needed to be transmitted before it tries to find a route to destination. AODV being a reactive protocol only keeps a routing table for the nodes directly adjacent to itself until a longer route is needed. Using this methodology allows for less network traffic to be broadcasted in times where the network is otherwise idle. [1] On the contrast there will be a slight delay when sending to a new node while it attempts to find the best route upon attempting to send.

2) Proactive: Each node in a proactive routing protocol such as DSDV will attempt to establish a best route to every other node in the network before any messages can begin to pass. [1] This will create a flood of network routing traffic to be broadcasted in the network just to keep a current picture of routing topology. The advantage of this style of protocol is that at any given time a message can be instantly sent to any reachable destination. A reactive protocol would first need to find out if that node is even reachable before it can attempt to send real traffic.
C. DARS Background

DARS provides a simulation environment for MANETs. The simulation environment has been designed to allow users to interact with mobile network to experiment and learn about different routing protocols. The simulation environment enables users to replay simulations with, or without, modification.

DARS is implemented using a two-tier architecture which isolates Simulation Engine from the Graphical User Interface (GUI). The Simulation Engine further isolates the routing protocol logic into separate modules. This enables additional protocols to be added. The two tiers communicate using Events. The Event Handler allows the different parts of the application to communicate. The GUI and the core Simulation Engine pass Events as the sole means of communication. The Simulation Engine handles the core computation of the simulation while passing output Events back to the GUI to be displayed. [2]

Protocols in DARS are implemented as modules within the Simulation Engine and must handle events that are sent to them to fulfill the construct of the application design. This enables new protocols to be easily added to the Simulation Engine and the greater DARS application.

By default DARS implements two routing protocols, Ad hoc On Demand Distance Vector (AODV) from RFC 3561 [3] and Destination-Sequenced Distance-Vector Routing (DSDV) as described by Perkins and Bhagwat [4].

1) DARS Features: DARS was developed to be a feature rich application. One of the primary feature goals of DARS was to be platform independent. This feature led to the cross platform capabilities that enable DARS to be accessed by a greater community. Additional high level features include:

- Intuitive Interface with Realistic Visualizations
- High Granularity of Node Control
- Flexible Topology Configuration
- Extensive Logging Capabilities
- Simulation Replay
- Pre-canned Scenarios
- Pre-canned Challenges
- Multiple Simulation Execution Modes including Real-Time User Interaction
- Real Time Routing Tables
- Extensibility via an exposed Application Programming Interface (API)

D. Education Through the Use of Games

It is widely known that the best way to teach someone is to create an experience that is engaging. Requiring a user to interact and respond keeps the participants focused on the topic at hand. [5] The DARS simulator strives to create an interactive experience that entices users to want to understand more about ad hoc routing. The use of challenges helps engage users to figure out a puzzle like scenario in order to solve a problem. The users must learn about how each protocol functions in detail in order to solve each challenge. After learning how each protocol functions, the next stage of learning that DARS try to fill is solving the problems presented with the default protocols included. The DARS simulator includes extensive documentation and examples to extend or create a new protocol. The simulator was designed from the ground up to make adding a new protocol all about how the protocol works and not about how to fit it into the simulator.

E. Security and Ad Hoc Routing Protocols

Ad hoc networks face many security threats that traditional routing environments do not face because of its centralized network infrastructure. In an ad hoc network the users act as the sender, recipient, and the router for other nodes in the network. This gives users in the network a lot of power and control over the network they belong to. Users can potentially disrupt, change, or collect network routing information and critical user information. The following sections briefly describe some of the many types of attacks that can be employed in these non-centralized network environments.

1) Message Tampering Attack: The message tampering attack in mobile ad hoc networks poses a serious security risk in the real world. In a normal wireless network all nodes communicate directly with a wireless access point. These messages can be intercepted by other users within wireless range. However, typically these access points employ some type of wireless security such as WPA. This keeps other users from viewing their peers’ network traffic. In ad hoc networks each user must rely on their peers around them to relay a message. This means they need to be able to read certain parts of the message to be able to know how to route it. The actual contents of the network packets can be encrypted to hide message information, but distributing an encryption key can be difficult to do when you rely on the same potentially malicious nodes to transfer your key. Not only can the contents of messages be changed but also packet header information containing network critical information such as destination, hop count, and sequence number can also be manipulated causing disruption of the network [6]. Of the two protocols that DARS implements neither was required to implement any form of protection for the message header or payload, thus enabling malicious network users to tamper with packets traversing them.

![Fig. 1: The Message Tampering Attack](image)

In figure 1 Node A attempts to send a message to a distant node. This message must be sent via its neighboring node, Node B. Node B is able to change the contents of Node A’s message before transmitting it further. The recipient of Node...
A’s message is unaware that the message has been changed. Additionally, it is possible that the distant node’s reply back to Node A can also be changed by Node B.

2) Message Dropping Attack: Message dropping attacks are implemented by a malicious node by dropping some or all messages that pass through it to artificially degrade network reliability. Under normal operating conditions in an ad hoc network a node will need to pass information to its peer nodes to establish routing tables to later pass real information. As illustrated in figure 2, a malicious node utilizing a dropping attack will pass this routing information around normally in order to construct its own routing information as well as make itself known in the surrounding network. As nodes begin to send real message information around the network however the malicious node will drop some or all of the traffic while continuing to respond to route information traffic. This will cause an artificial black hole for real message information. These black holes in the network can further cause node, or network segment, isolation from the greater network if the malicious node is strategically located [7].

![Fig. 2: The Message Dropping Attack](image)

3) Message Replay Attack: The message replay attack can be used in conjunction with the message dropping attack, but it doesn’t necessarily need to. In a normal network a node will receive a message to be passed to another node and , if the current routing table permits, immediately send the message on without any further action. A malicious node however can store the message and resend it at a later time. The node can drop the original message and send the new message at a large delay creating an artificial delay in the network or it can send the original message and the new message as a second copy confusing the recipient. On an individual message base this can cause the receiving node an inconvenience, but on larger scale the message replay attack can be used as a form of route disruption.

![Fig. 3: The Message Replay Attack](image)

4) Fake Hop Count Attack: The fake hop count attack can be used to direct network traffic away from or towards a malicious node. The malicious node in this attack will lie about the hop counts to other nodes in the network. Under proper routing protocols a node will choose the shortest route to a destination based on the hop count to that destination. As routing tables are built only the best routes to each node are kept. If a malicious node is attempting to direct all network traffic through itself in order to drop or read network traffic it can fabricate a new hop count. This could be done to indicate to other nodes that every other node is only one hop away. Other nodes surrounding this malicious node will then begin to forward messages through the route disrupting node. Conversely, nodes can also fabricate artificially high hop counts to change the routing path in the network. This would be helpful for the malicious node to save its own bandwidth, but bad for the overall network performance by causing more traffic to flow through potentially worse routes.

![Fig. 4: The Fake Hop Count Attack](image)

In figure 4, Node A forwards route request to Node B requesting information about a distant node. Even if Node B has a legitimate route in its route table it will replay back to Node A with a fake hop count. This faked hop count does not directly change Node B’s route table.

5) No Timeout Attack: The no timeout attack is used by malicious nodes to lie about the presence of other nodes in the network. Under normal operating conditions in a network when a node comes within range of other nodes its presence is announced in a broadcast message and other nodes are notified that the new node should be added to their respective routing tables. Consequently when a node leaves the network and it no longer responds to network requests it is deleted from all other node’s routing tables based on a set timeout. However, a malicious node can exploit this concept by lying about being able to communicate with a node that has left the network by never expiring the route in its own routing table. When a neighboring node requests all the routes that the malicious node knows of it will respond that the missing node is still there and able to be reached through the missing node. This allows a malicious node to continue to gather messages for a node that has already left the network.
III. SIMULATOR ENHANCEMENTS

The DARS simulator has been enhanced to include network attacks that were described in the above sections. The implementation of these enhancements touched every area of the DARS application. The new functionality was implemented in a way that if additional protocols are added to DARS only the protocol can implement the malicious features of the simulation without having to edit the rest of the DARS application.

A. GUI Enhancements

The GUI is the primary interface for users to interact with the simulation. The GUI was changed to add an intuitive way of setting up malicious nodes. A user may add one or more malicious actions for a node to take at any time before or during a simulation. This enables the user to experiment with combinations of attacks. This was done through the new Malicious Controls panel.

1) Malicious Node Controls: Malicious node controls were added to the DARS simulator to allow for a single node to be altered to behave maliciously. The node controls feature a check box for each type of malicious attack as well as spin box that allows customization of of the hop override attack. This feature allows the user to specify the number of hops the node should say every other node is away from itself. Each of the node configuration items can be selected independently without conflict. Since the original version each menu item in DARS has been given a tool-tip with a brief explanation of the use of each function. When a node is flagged as malicious in DARS it is turned a bright red to easily identify the rogue node in the network.

2) User Feedback: The user is provided feedback on these configurations through the identification of malicious nodes by color. When a node has been selected to perform malicious actions it is highlighted in red so that is easily tracked while a simulation is in progress.

B. Input and Output Event Handler Enhancements

New event types for malicious actions were created. This enables the simulation engine to directly interface with the node interface about malicious attribute changes. All of these events are also recorded via the logger.

C. Logger Enhancements

The DARS log engine was modified to process the new event types. These event types are capable of being processed through the log reader on simulation replays, thus enabling the users to re-watch an attack and analyze it.

D. Protocol Enhancements

All malicious attack types implemented in DARS simulation engine were also implemented in the AODV and DSDV protocols. This enables users to compare the two different protocols and how they handle various attacks. Future protocols can also implement these new attack event types without the need to modify the other areas of the application.

E. Scenarios Enhancement

In addition to enabling users to create and save their own simulations, DARS has been enhanced to supply pre-canned scenarios to demonstrate various attacks. These scenarios can be changed and built upon by the user before being optionally saved to an external log file for later replay.

IV. SCENARIOS AND EXPERIMENTATION

In order to demonstrate how these attacks can be carried out in ad hoc networks, DARS provides scenarios that can be played out at any point. These scenarios can be used with any protocol that is built into DARS. By default just AODV and DSDV are included. Each scenario can be loaded in locked mode or interactive mode. In interactive mode the
nodes in the scenario can be moved and manipulated to alter the outcome of the replay. In locked mode only the preset actions are performed on the nodes in the environment. The aim of these scenarios is to teach others about the various vulnerabilities of MANETS through demonstration. The use, creation, modification, and replay of scenarios within DARS enables students, educators, and researchers the ability to interact with a network and manipulate it to see what affect various change have to a network. The ability to save these scenarios and share them is also supported.

A. Example Attack Scenarios

In the following sub-sections each included new attack method’s scenario is explained. These scenarios are available to all users via the main menu. Each of the attacks that was implemented in DARS were used to determine their affects on each of the two routing protocols that are included with DARS. The results that were found are discussed in the following sections.

1) Message Tampering Attack: The message tampering attack in DARS will allow network control traffic to flow through the malicious node without issue. When a narrative message that contains a real payload is detected it is modified before being forwarded on to the next node in the network. This behavior is common between AODV and DSDV without any distinctive differences.

2) Message Dropping Attack: This message dropping attack is fairly straight forward in comparison to the other attacks. A malicious node will continue to send and receive control messages that are related to building routing tables. However when an actual message with a payload is sent it will be immediately dropped. The characteristics of this attack do not vary from reactive and proactive protocols. Therefore both AODV and DSDV behave in the same manner when the attack is applied.

3) Message Replay Attack: The message replay attack is very similar from AODV to DSDV. Both attacks respond similar to the dropping attack in that they both will simply send a message many hops after receiving it the first time. Neither protocol has an advantage over the other while using this type of attack.

4) Fake Hop Count Attack: The fake hop count attack behaves very differently from AODV to DSDV. It is much easier to accomplish the attack when using a proactive routing protocol such as DSDV. This is due to the fact that in a reactive protocol the routing table is only stored for nodes directly adjacent to each node. In a proactive routing protocol the routes to every other node in the network are stored at all times.

   a) AODV: Since AODV is a reactive routing protocol only the nodes directly adjacent to each node are stored.

In order to for a node to lie about the hop count it must first discover the node in question before replying to the originating requester. This gives other nodes a chance to reply to the originating requesting node before the malicious node has a chance to respond. However, if the malicious node has a recently cached route in its own routing table from a previously sent message it can quickly respond to requesting originator with false information about the route. That doesn’t necessarily mean that the other nodes in the route information, so the message may or may not make it to its final destination.

   b) DSDV: This attack is much easier in DSDV because it will store the complete best route to every other node in the network. This allows a malicious node to give incorrect information out to every other node and quickly corrupt the entire networks routing tables. This can ensure that the malicious node can intercept almost all information in the network and combine other types of attacks such as the dropping attack to cause a crippling black hole attack.

5) No Timeout Attack: The no timeout attack is equally effective in both AODV and DSDV. Both protocols are susceptible to the attack because they rely on a response from a peer node to tell them about the existence of its neighbors.

   a) AODV: Since AODV is a reactive routing protocol all the nodes will expire the route to the missing node that has left the network. Only when requesting a route to this missing node will the malicious node respond that it has a still valid route. If the other nodes in the network were not aware of the node that has gone missing, they will not know to request a route for it.

   b) DSDV: DSDV being a proactive routing protocol attempts to build a routing table for all nodes on the network that is kept up to date at all times. This means that the malicious node has a chance to tell all other nodes in the network that the missing node is still in the network. This means that new nodes into the network will be incorrectly informed of the missing nodes existence.

B. Challenges

Since the goal of the DARS simulator is to provide a teaching aide to computer science students, another type of scenario has been added to the simulator called challenges. Challenges differ from scenarios in that they are intended to be interactive whereas the previous scenarios are meant to be watched as a demonstration without hands-on interaction until completion. These challenges provide a way for students to use their knowledge to execute a network attack. DARS provides two challenges pre-canned into the simulator.

1) Challenge 1: This challenge asks users to create a black hole attack using one of the nodes given in the network. The goal of the back hole attack is to force all network traffic to be routed to a single point in the network where the traffic is dropped. This causes the integrity of the network to degrade until it is rendered useless. In the given scenario the users are
Fig. 7: The DARS Simulation Software Demonstrating a Malicious Attack

not allowed to change the topology of the network to make the scenario easier. The users are only allowed to use the malicious controls to create their attack. This challenge can be performed for any protocols included in DARS. By default this includes DSDV and AODV.

2) Challenge 2: Challenge 2 asks users to create a Denial of Service attack using one of the nodes given to drive all messaging traffic through another node in the network. In real life this would consume all of the victim node’s resources and cause network traffic to degrade significantly. Like challenge one the nodes are not supposed to be moved in order to change the topology of the network.

V. Conclusion

DARS has shown flexibility and extendability as new features have been added. These new features were used to demonstrate some of the many problems that mobile ad hoc networks face during their emergence into the real world market. Not only has the DARS simulator proven to be friendly to extend and upgrade, the simulator has also proven to be a useful tool with others around with world, with over 1,300 downloads from sourceforge.net alone from many different countries, DARS has become known outside of the local College level. With the addition of new features and functionality it should become even more successful in the proliferation of mobile of ad hoc networks.

A. Limitations

The DARS routing simulator although rich in features and functionalities still has its limitations. The simulator does not take into consideration power consumption and bandwidth limitations. These features were not implemented because of time constraints and complexity. This simulator’s intended purpose was to focus on the inter-workings of various routing protocols, not the limitations of hardware and environmental factors.

DARS also is a network routing simulator and only focuses on the network layer of each routing protocol. The lower and upper layers of the OSI model are not taken into consideration when running simulations on DARS.

The challenges included with the simulator are left up the educational instructors to demonstrate a correct solution. The challenges themselves do no include the a pre-canned solution because multiple solutions are possible.

VI. Future Work

Moving forward some of DARS limitations could be addressed as were discussed previously. The simulator engine could be redesigned to take into consideration some outside environmental factors such as power consumption, bandwidth limitations, and packet corruption. These factors would allow for an even more accurate to real life simulation.

New protocols could also be added for demonstration purposes. Many new protocols are developed each year while the ad hoc networks begin to gain popularity. These protocols include SAODV [8], AOMDV [9], and AODVM [10] which
are based on the AODV protocol and MDVZRP [11] which is a completely separate protocol. These could include protocols like SAODV that provides some protections against some of the malicious attacks described in this paper.

After initial feedback is acquired from users of the simulator, new and more advanced scenarios can be included with the simulator by default. These would be tailored to support the exact needs of the educators. For example the challenges could support multiple solution examples that could be revealed with a special unlock code set by an instructor.

ACKNOWLEDGMENT

A special thanks to our professors at Hood College, George Dimitoglou and Ahmed Salem, as well as the past developers of the DARS project, namely Michael Moorman. Michael was an essential part of the orginal creation of the DARS simulator.

REFERENCES