Security Issues In Mobile Ad hoc Network Routing Protocols

Philip Huynh

phuynh@uccs.edu

Abstraction

Mobile ad hoc network (MANET) is gaining importance with increasing number of applications. It can be used for emergency and rescue operation, conferences and campus settings, airport and car networks, and other more. Multi hop routing protocols are designed for MANET to provide services same as the layer three, Networking, in the OSI network model. Because the multi hop routing protocols are used to exchange packets between mobile nodes, they are usual the target for the attacking to the MANET. Adversary can increase the adversarial control over the communications between some nodes, decrease the quality of services of the network, or increase the energy consumption of some nodes by having the compromised nodes to attack the routing protocols. The routes between some nodes could be deleted or changed from the original purposes of the routing protocols. This report expresses some security issues in the multi hop routing protocols of MANET as well as the countermeasures against the attacks. Some attacks were simulated on the computer to help research the countermeasure methods.

1. Introduction

MANET is an autonomous, self-configuring system of mobile devices (laptops, smart phones, sensors, etc.) connected by wireless links. Each node operates as both an end-system and a router. The MANET characteristics are mobility and dynamic topology, bandwidth-constrained, energy-constrained, and prone to security threats. MANET was initially designed for military applications, but with the increase of portable devices as well as process in wireless communication, MANET is gaining importance with increasing number of applications. It can be used for emergency and rescue operation, conferences and campus settings, airport and car networks and other more.

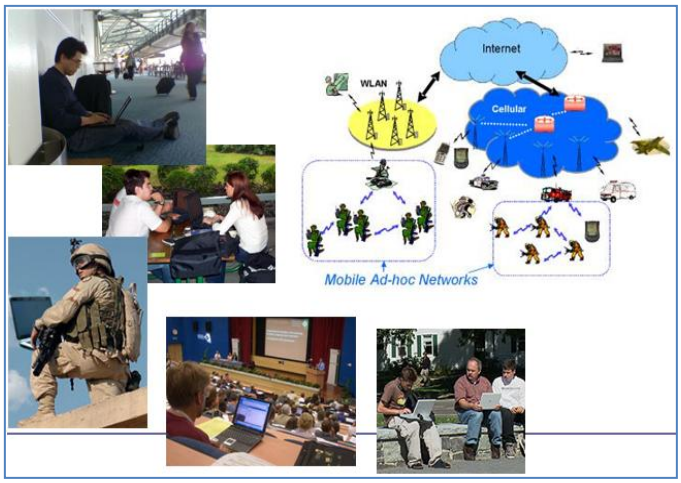

Figure 1 - MANET applications

As in [1] the ad hoc network routing protocols can be classified into topology-based protocols and position-based protocols. Topology-based protocols are based on traditional routing concepts, such as maintaining routing tables or distributing link-state information, but they are adapted to the special requirements of mobile ad hoc networks. Position-based

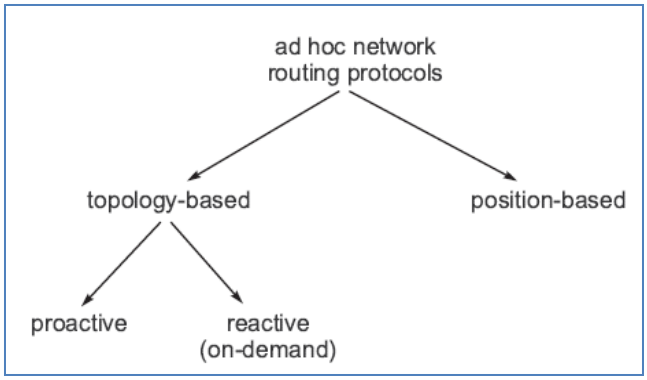

Figure 2 – The classification of ad hoc network routing protocols

protocols use information about the physical locations of the nodes to route data packets to their destinations (e.g. GPSR, GOAFR, DREAM, and LAR). Topology-based protocols can be proactive (e.g. DSDV, OLSR) or reactive (e.g. AODV, DSR). Proactive protocols try to maintain consistent, up-to-date routing information within the system. In contrast to this, reactive protocols establish a route between a source and a destination only when it is needed. For this reason, reactive protocols are also called on-demand protocols.

An example of routing protocol Dynamic Source Routing Protocol (DSR)

DSR is on-demand source routing protocol. It has two components:

Route discovery – this component is used only when source S attempts to send a packet to destination D. It is based on flooding of Route Request (RREQ) and returning Route Replies (RREP).

Route maintenance - this component makes source S able to detect route errors (e.g., if a link along that route no longer works)

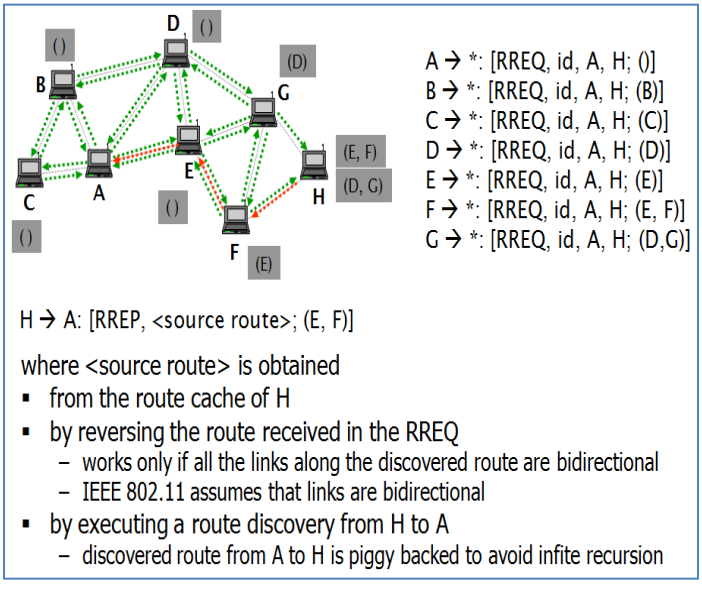

Figure 3 – The illustration of Dynamic Source Routing Protocol

In the following section, I will discuss the attack mechanisms in the MANET. Section 3 deals with the types of attack. The countermeasures are discussed in section 4, followed by an

example about the secure routing protocol in section 5 – The Secure Routing Protocol (SRP). Section 6 gives a simulation of the Gray hole attack in the multi hop routing protocol for Wireless Sensor Network. And the conclusion is in the section 7.

2. Attack Mechanisms

In MANET, the attack mechanisms can be classified as the following categories:

Eavesdropping, replaying, modifying and deleting the control packets – The compromised nodes can modify or delete the control packets as in [1] or the routing information as in [3].

Fabricating control packets containing fake routing information (forgery) – The compromised nodes can create or modify the control packets that will contain the fake routing information.

Fabricating control packets under a fake identity (spoofing) – The compromised nodes can create or modify the control packets that has a fake identify.

Wormholes and tunneling – A wormhole can be setup with two compromised nodes that communicate together out-of-band as in figure yyy. In the case of a tunnel, the two compromised nodes exchange control packets using the existing route in the network, look at Figure 4.

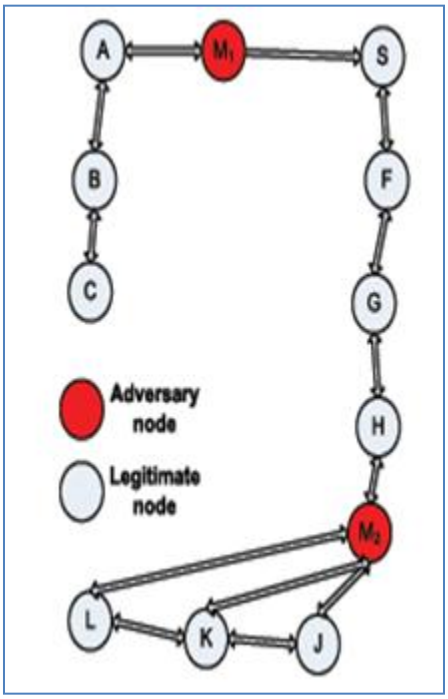

Figure 4 - The Tunnel in MANET

Rushing – As in [2], a rushing attack is a malicious attack that is targeted against on-demand routing protocols that use duplicate suppression at each node. An attacker disseminates ROUTE REQUESTS quickly throughout the network, suppressing any later legitimate ROUTE REQUESTS when nodes drop them due to the duplicate suppression.

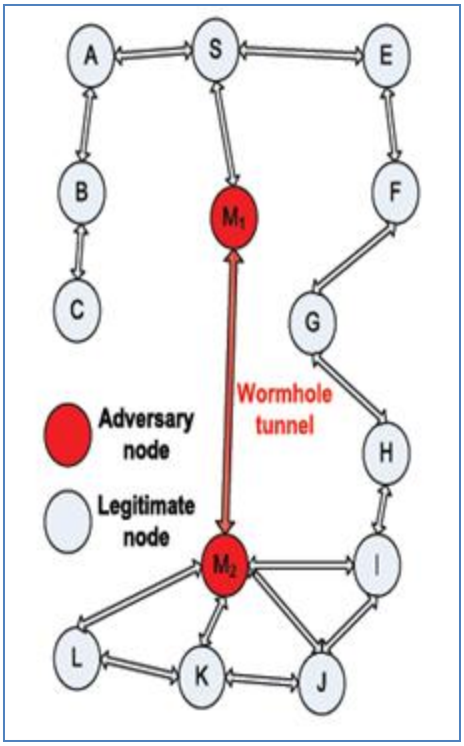

Figure 5: The Rushing with wormhole in MANET

3. Type of Attacks

As in the [1], using the above mechanisms, an adversary can mount the following types of attacks against routing protocols:

Route disruption – The adversary prevents a route from being discovered between two nodes that are otherwise connected. Attack mechanisms that can be used to mount this attack: Dropping route request or route reply messages on a vertex cut; Forging route error messages; Combining wormhole/tunneling and control packet dropping; Rushing.

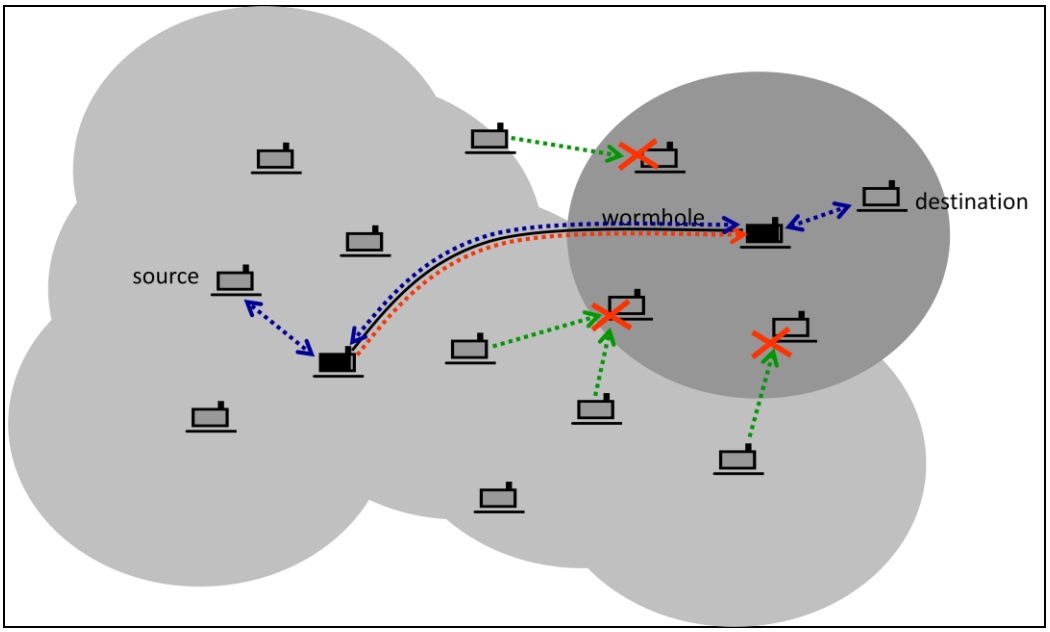

Figure 6: An example of Route disruption attack using Rushing

Route diversion – Due to the presence of the adversary, the protocol establishes routes that are different from those that it would establish, if the adversary did not interfere with the execution of the protocol. Attack mechanisms that can be used to mount this attack: Forging or manipulating routing control messages; Dropping routing control messages; Setting up a wormhole/tunnel;

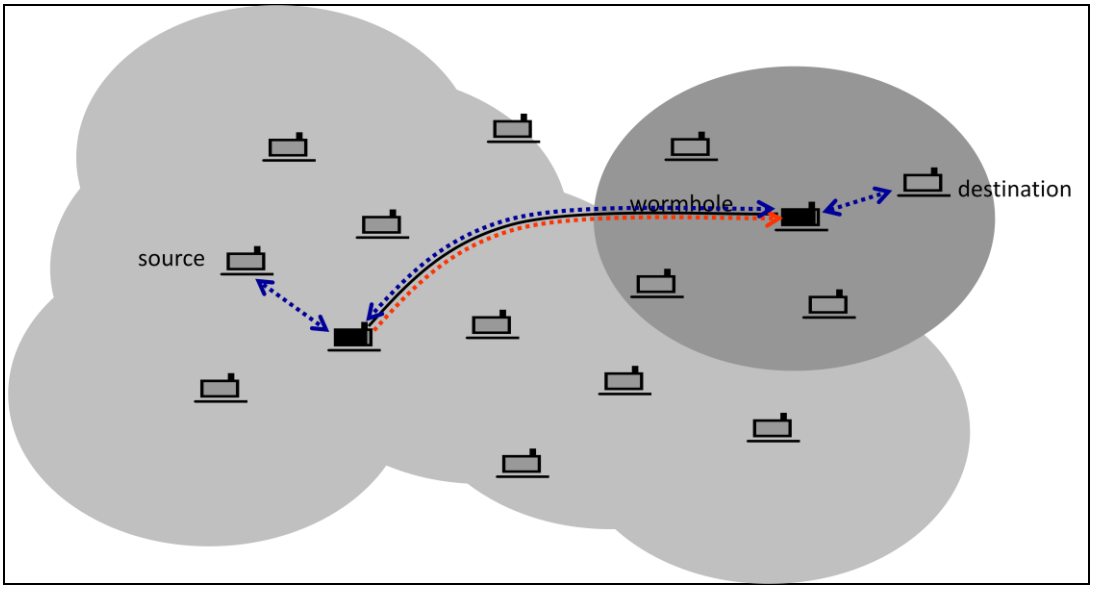

Figure 7: An example of Route diversion attack using Rushing

Creation of incorrect routing state – This attack aims at jeopardizing the routing state in some nodes so that the state appears to be correct but, in fact, it is not. Data packets routed using

that state will never reach their destinations. Attack mechanisms that can be used to mount this attack: Spoofing, forging, modifying, or dropping control packets.

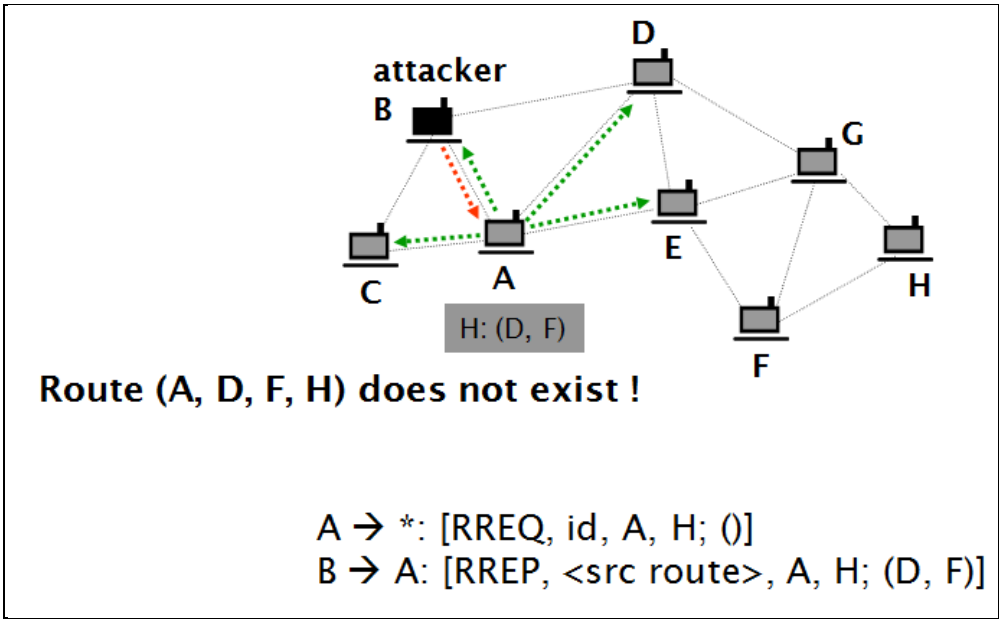

Figure 8: An example of Creation of Incorrect routing state

Generation of extra control traffic – This attack aims at injecting spoofed control packets into the network. It is aiming at increasing resource consumption due to the fact that such control packets are often flooded in the entire network

Setting up a gray hole – An adversarial node selectively drops data packets that it should forward. To do that, the adversarial node participates in the route establishment. When it receives data packets for forwarding, it drops them. It can be combined with wormhole/tunneling.

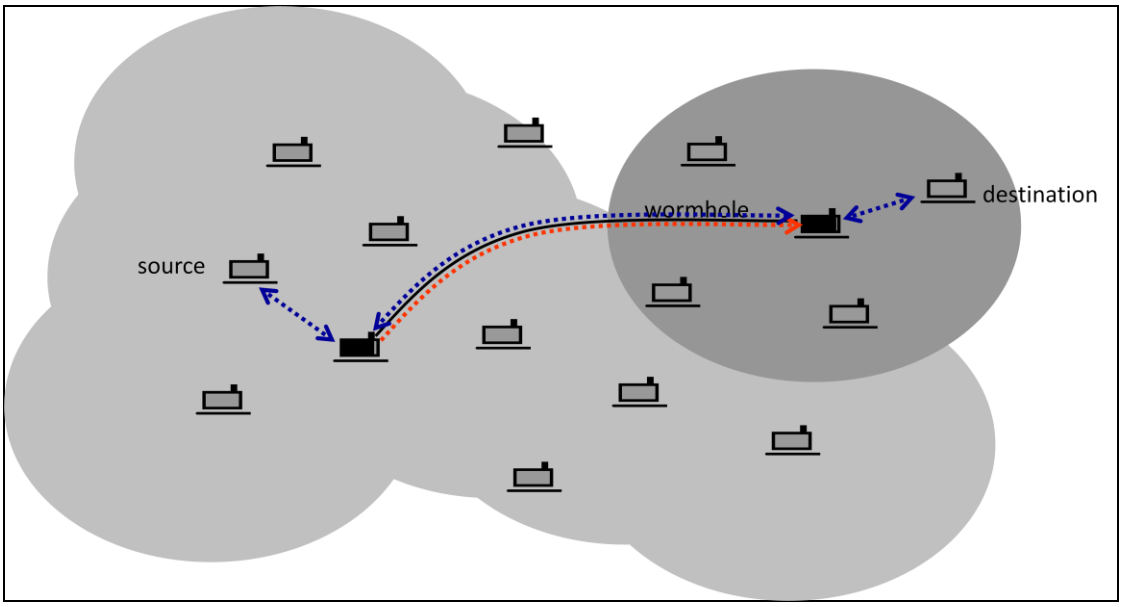

Figure 9: An example of Setting up a Gray hole attack

4. Countermeasures

There are some proposed techniques that can be used to defend against the multi hop routing protocol attacks as in [1].

Authentication of control packets – Control packets should be authenticated by their originators. Authenticity should be verifiable by the target of the control packet. Moreover, each node that updates its routing state as a result of processing the control packet must be able to verify its authenticity. Each node that processes and re-broadcasts or forwards the control packet must be able to verify its authenticity. Ramkumar proposed an efficient broadcast authentication scheme [8].

Protection of mutable information in control packets – Each node that adds information to the packet should authenticate that information in such a way that each node that acts upon that information can verify its authenticity. The added information can be categorized in traceable additions (e.g. adding node identifiers), and untraceable additions (e.g. increasing the hop count). The traceable additions can be authenticated with re-signed the entire control packet by each node that modifies it. But with the untraceable additions, there is no perfect solution exists. For example, the hop count can be increased uncontrolled by the adversarial nodes.

Detecting worm holes and tunnels – Wormhole detection is a complicated problem. The mechanisms can be categorized into centralized and decentralized approaches. In centralized approaches, the central entity will gather the information about the network and construct a

model of the entire network. Then the central entity tries to detect inconsistencies (potential indicators of wormholes) in this model. In the decentralized approaches, each node constructs a model of its own neighborhood using locally collected data. The each node tries to detect inconsistencies on its own. In the second approach, there is no need for a central entity, but nodes need to be more complex.

Combating gray holes – There are two approaches. The first one is using multiple disjoint routes. This approach increases the robustness of the routing protocol but it also increases resource consumption. The second approach is "Detect and react". This approach monitors neighbors and identify misbehaving nodes. The routes will not contain the misbehaving nodes.

5. Secure multi hop routing protocols

In [1], there is a list of some secure multi hop routing protocols. Each secure routing protocol can defend against some above attack types, but there is no perfect secure solution. There are some well-known secure routing protocols, such as SRP, Ariadne (on-demand source routing), S-AODV (on-demand distance vector routing), SEAD (proactive distance vector routing), SMT (multi-path routing combined error correcting), ODSBR (source routing with gray hole detection).

To illustrate how the secure multi hop routing protocol work. Let's analyze an existing secure routing protocol; its name is Secure Routing Protocol (SRP).

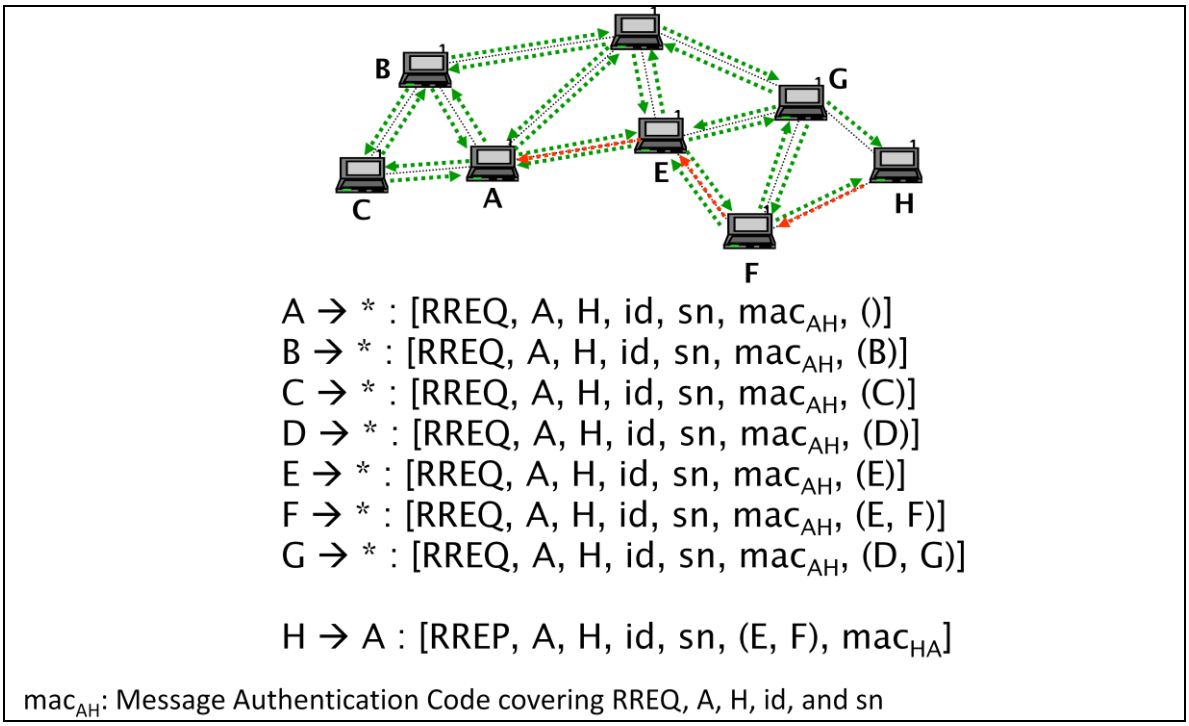

Figure 10: An example of Secure Routing Protocol (SRP)

Secure Routing Protocol (SRP) is a secure variant of DSR. It uses symmetric-key authentication (MACs) between the source and the target nodes. There is only end-to-end authentication. SRP is simple but it does not prevent the manipulation of mutable information added by intermediate nodes. Thus, this opens the door for some attacks, such as route diversion. However, some of those attacks can be thwarted by secure neighbor discovery protocols.

6. Simulation

Wireless sensor network (WSN) is a special type of MANET. In WSN the motes are not mobile like the MANET, but they are more limited in energy supply, CPU capability, and memory. WSN applications can be developed with the TinyOS platform that is open source software.

Some attacks to the multi hop routing protocols can be simulated in the TOSSIM software which is the simulation for TinyOS applications. As in [7], some multi hop routing protocols has been developed in TinyOS, such as Ad hoc On Demand Distance Vector (AODV), and Destination Sequenced Distance Vector (DSDV). In TinyOS, there is a multi hop routing protocol library called MultihopRouter component which is a tree-based collection routing type.

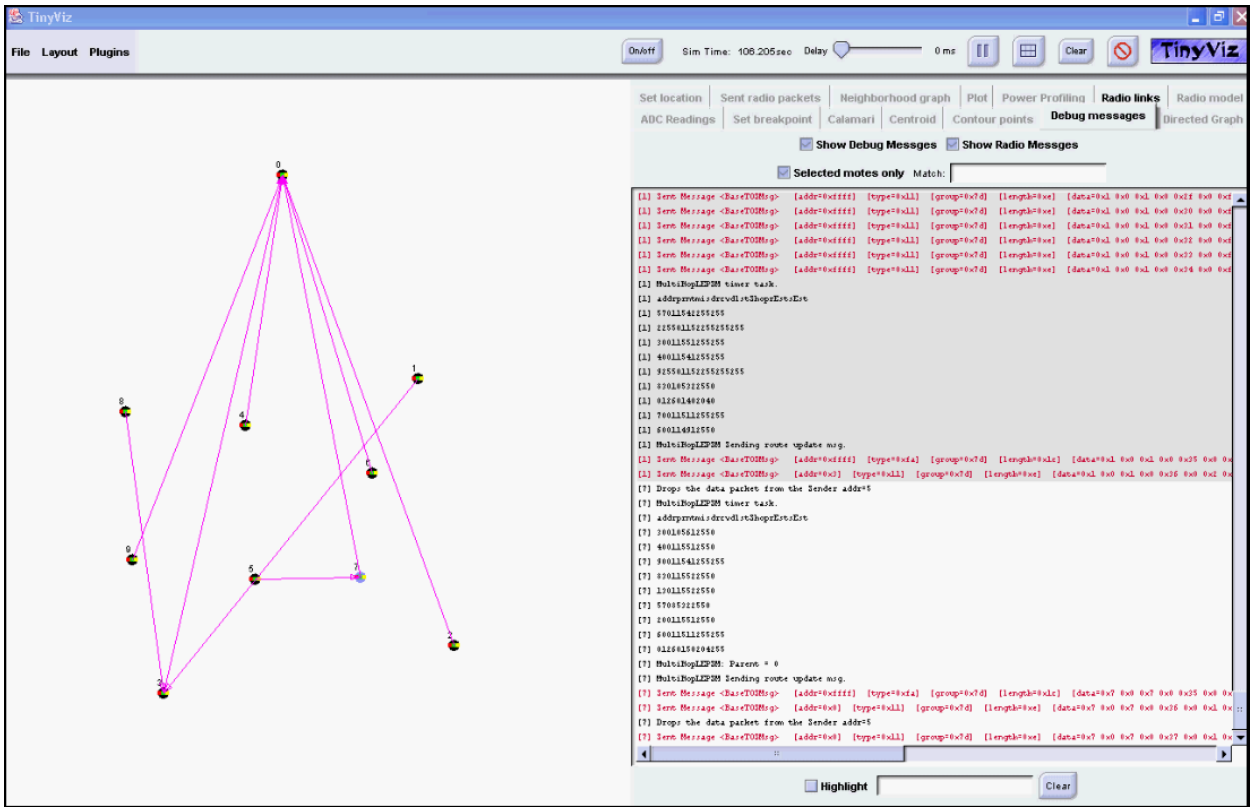

Figure 11: An illustration of Gray hole attack. The simulation was created using TinyOS, TOSSIM, and TinyViz. The Surge application was modified for this demo. The adversarial node drops all incoming data packets instead of forward them to the Base station.

As in [3], many WSN applications were not designed with the security in mind. The "Gray Hole" attack in [1] or "Selective Forwarding" attack in [3] was selected for the simulation. The Surge application in the folder"TinyOS.1.1.x/apps/Surge" was modified to simulate the "Gray Hole" attack. The compromised hop (or a mote) will drop all data packets instead of forward them to the Base station node (mote with id is zero). The simulation can be extended to defense against the "Gray Hole" attack by implementing the multi path disjoint routing protocol as in [1].

7. Conclusion

Routing is a fundamental function in networking, hence, an ideal target for attacks. Although the secure routing protocols have been proposed, they are not perfect and exploited. Many attacks can be prevented by authenticating routing control messages. It is difficult to protect the mutable part of control messages.

Some multi hop routing protocols and attacks has been simulated on computer for research using the TinyOS, TOSSIM, and TinyViz software.

References

[1] Levente Buttyan and Jean-Pierre Hubaux, “Security and Cooperation in Wireless Networks”, Version 1.5.1 July 27, 2007.

[2] Yih-Chun Hu and Adrian Perrig, “A Survey of Secure Wireless Ad hoc Routing”, IEEE Computer Society 2004.

[3] Chris Karlof, David Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures”, Elsevier B.V. 2003.

[4] Philip Levis, Nelson Lee, Matt Welsh, and David Culler, “TOSSIM: Accurate and Scalable Simulation of Entire TinyOS Application”.

[5] Philip Levis and Nelson Lee, “TOSSIM: A Simulation for TinyOS Networks”, September 17, 2003.

[6] Philip Levis, “TinyOS Programming”, June 28, 2006.

[7] Shailesh A Notani, “Performance Simulation of Multihop Routing Algorithms for Ad hoc Wireless Sensor Networks Using TOSSIM”.

[8] Mahalingam Ramkumar, “An Efficient Broadcast Authentication Scheme for Ad hoc Routing Protocols”, IEEE ICC 2006.