# Study on the Wireless Ad Hoc Network Secure Routing Based on the SAR Technology

Peng Li

College of Information Engineering, Taishan Medical University

Tai'an 271016, China

E-mail: lipeng@tsmc.edu.cn

Received: February 22, 2011 Accepted: March 25, 2011 doi:10.5539/cis.v4n3p151

**Abstract**

In this article, the SAR (Security-Aware Routing) technology is applied in the AODV (Ad Hoc On-demand Distance Vector) routing protocol, the AODV is modified as viewed from security performances, the wireless Ad Hoc routing protocol with secure consciousness could be realized, and the secure routing protocol (SAR-AODV) is simulated in the OMNet++ simulation environment based on the platform of Windows 2003.

**Keywords:** Ad Hoc, SAR, Secure routing

## 1. Introduction

Without fixed infrastructure, wireless Ad Hoc network is a new wireless communication mode, and each mobile node has both the function of router and the function of host computer, and all nodes are mobile and dynamically link with other nodes. It is a kind of networking mode logically. As same as wire network, the wireless Ad Hoc network is often harmed by the attacks from exterior hostile nodes and the secrete leakage from interior nodes, and the mobile character of the Ad Hoc network will amplify the influence of attack, so the security is one of hot research points for the Ad Hoc network.

## 2. Secure studies of wireless Ad Hoc

### *2.1 Intrusion detection*

Wireless Ad Hoc network has many characteristics such as multiple dynamic topologic changes, lacking in centralized monitoring and management points, and lacking in defense, so it is easier to be attacked. The intrusion detection such as encrypting and identifying is used to protect the network operation, and it is necessary for any high-effective network. But many intrusion detection technologies come from fixed wire network, and they are not applied in the new environment. And the detection could not defend the leakage node, because this kind of node carries secret key. Therefore, it is an important challenge to detect the intrusion effectively.

### *2.2 Secure routing*

In the Ad Hoc network, the routing protocol should defend the topology update and any kind of attack. Being different with wire network, the routing information in the Ad Hoc network will become the target where the hostile nodes attack the network. For the Ad Hoc routing protocol, there are two threats. The first one comes from exterior attacking nodes, which include inserting wrong routing information, resetting old routing information, and misreporting routing information. Through these methods, attackers could successfully divide the network or increase additional flow load, which would make the system retransmit the routing information or induce invalid routing. The password mechanism such as encryption and digital signature could defend exterior attacks. The second threat comes from compromised leakage nodes, and these nodes may transmit hostile routing information to other nodes, because these compromised leakage nodes may produce legal signatures, so this threat is more difficult to be detected, with larger harm.

The existing routing protocol is good at dealing with dynamic topology, but its effect on security detection is not ideal. One of solutions is to design the secure routing protocol with many characteristics such as adapting dynamic topology, the nodes which could be easily attacked, limited computation ability, and capacity limitation.

### *2.3 Secrete key management service*

Traditional encryption mechanisms such as digital signature and public key still plays very important role in the Ad Hoc network. All these mechanisms all need the service of secret key management. Generally, the secret key

management service is the trusted entity based on certification authority (CA). In the Ad Hoc network, it is very danger to use single CA to establish the secret key management service, because single CA would be the key which is easy to be attacked in the network. If CA is damaged, the security of the whole network will collapse. It is very important to establish the trusted secret key management service in the Ad Hoc Network.

## 3. Wireless Ad Hoc network secure routing based on SAR technology

### *3.1 SAR technology*

SAR technology integrates the security attribute into the Ad Hoc route discovery as a parameter, so the security becomes a negotiable parameter to enhance relative route discoveries in the Ad Hoc network protocol.

Ad Hoc network adopts logical network mode, and it emphasizes that the mobile terminals in certain area could dynamically establish interconnect network, independent of network infrastructure. Most Ad Hoc routing protocols have the character that absolutely trusts neighboring nodes and transmit package among nodes based on this character. This "innocent" trust mode makes some hostile nodes can destroy the Ad Hoc network by many measures such as inserting wrong routing update, resetting old routing information, and distorting routing update. Though fixed wire network would be attacked by these measures, but the characteristic of the wireless Ad Hoc network would amplify the influence of attack, and fail the protection measures. In the wireless Ad Hoc network, the communication among nodes is completed based on the support of the routing protocol, and the performance of many traditional mobile Ad Hoc routing protocol is good in the dynamics, but the security is deficient. By the example of the Ad Hoc network in the battlefield communication demanding on the routing level, the designer of SAR technology described the necessity to strengthen the security consciousness on the routing levels (seen in Figure 1).

In Figure 1, generals denote two mobile nodes which want to communicate, and officer's security performance is better than soldier's. To establish one communication route between two generals, the shortest route through one soldier will be found according to general on-demanding Ad Hoc routing protocol, but in some situations, generals would worry soldiers will leak information, so they want to find a route only passing officer to transmit information, because even generals encrypt the communication information, the enemy still would know the communication fact through the soldier node with less security, which will also induce certain harm. Therefore, the SAR technology is used to improve the routing protocol.

By the SAR technology, generals in Figure 1 would come round the soldiers with less security consciousness, and establish one more safe route only passing officers. If the protocol could find thus a route according with the security requirement, it will establish the dialog between two generals, and if the protocol could not find thus a route to accord with the security attribute or the protection quality, it will inform the sender that the route establishment fails and renegotiate the security level.

From above example, sender or protocol sponsor could confirm the level of demanded "protection quality" of the transmitted data package by embedding the security attribute into the route discovery of the protocol. Furthermore, the protection quality provided by the route will directly influence the security of the data package on certain one special route. At the same time, the route update and the routing transmission information will be protected by this technology.

### *3.2 AODV protocol*

AODV is a kind of reacted routing protocol, i.e. only when demanding, the node will start the route discovery process, and generally, the route among those nodes without communication will not be kept necessarily.

When one node needs communicate with another node, if the route to this destination node doesn't exist in the routing table, the routing discovery process needs starting to find a route to the destination node. First, the source node broadcasts a route request (RREQ) message to all neighboring nodes which broadcast RREQ to neighboring nodes successively until this message has been transferred to the destination node or the middle node which has the route with the destination node. In this process, the middle node passed every time will input the sign ID of the upper node into the routing table and establish a reverse route from this node to the source node. Finally, the destination node or the middle node which has the route with the destination node transmits the route reply (RREP) message to the source node, and the route discovery process from the source node to the destination node ends. When the source node moves, it will restart the route discovery algorithm, and if the middle node moves, its neighboring nodes will find the linkage failure and send the linkage failure message to the upper node until to the source node, and then the source node restart the route discovery process according to the situation.

*3.3 SAR-AODV*

By the SAR technology, the security attribute is embedded into the RREQ package of the AODV protocol, which will change the transmission of the protocol about the RREQ package. When the middle node receives these RREQ packages with special security attribute or trust level, it will first check whether it has the security level indicated in the RREQ package or the demanded authority or trust level, and if this node could not provide the demanded security level, it will discard the RREQ package, and will not transmit it outside, and if it has the demanded security attribute, it will transmit the RREQ package like common AODV protocol until the destination node is found. After the final destination node is found, the destination node will transmit a RREP package which will arrive at the source node according to the reverse route, and in this way, the route according with the secure standard will be established.

## 4. Simulation result

*4.1 Introduction of simulator*

OMNet++ is the object-oriented distributed event simulation tool developed by the School of Electronics and Information Engineering of Budapest University of Technology and Economics, and it can be used in the modeling and simulation of the communication protocol, the computer network multiprocessor and distributed system, and the management system.

Adhocsim is a kind of Ad Hoc network simulator designed by Nicola Concer of Bologna University in the environment of OMNet++ v2.2, and this simulator can describe the mobile Ad Hoc network in the area without barriers.

Every mobile node is defined as a complex module, and this composite module is composed by following simple modules including the physical layer, the MAC layer, the route layer, the application layer, and the mobile layer. The system structure is seen in Figure 2.

NS2 (Network Simulator 2) is the senior edition of NS modified by UC Berkeley's MASH research group, and it uses the TCL scripting language and the C++ language.

TCL (Tool Command Language) can provide a powerful platform, and generate application programs, protocols, and drivers which could orient many platforms. TCL interpreter interprets executed scripting language, and its implementation depends on the interior C function base of TCL. New C function could expand the order and function of TCL, and it is the scripting program design language with powerful expansibility.

TCL interpreter preliminarily analyzes the orders and program sentences inputted by user and transfers the corresponding function in the C function base to perform them and output the result.

*4.2 Simulation result*

NS2 and the Adhocsim simulator based on OMNet++ are respectively used to simulate SAR-AODV, and in the simulation of the Adhocsim simulator, the topology model, the node movement direction, and the node movement speed come from the assemblies of the simulator, and the simulation time (non-real time) is 5 min, and the topology model of NS2 simulation is seen in Table 1.

In Figure 4, the point 4 is sending the message of "Hello" to the point 2. On the one hand, OMNet ++ uses the round dots with different colors to denote different types of information, for example, the yellow denotes the transmitted message is RREQ, and the blue denotes RREP, and the green denotes Hello, which will make the simulation process become more clear. On the other hand, because the modularized characteristic of OMNet++, the implementation is more easy to operate comparing with NS2 simulator, because it should modify all documents coming down to RREQ and RREP.

In the implementation of protocol, the cLongHistogram class in OMNet++ is used to collect the data such as the size and type of the transmitted package in the simulation, and for each node, the histogram like Figure 5 could be obtained after the simulation. Figure 5 is the packet histogram of the node 0 in the whole simulation.

## 5. Conclusions

As a kind of self-created, self-organized, and self-managed network, Ad Hoc network has many advantages such as quickly flexible networking and node distributivity, and it is irreplaceable in many special domains such as war and disaster relief. In addition, because it needs not the infrastructure, and the most investment in network is in the user terminal, it is largely attractive for network operators. It can be used to quickly establish an access network (AN) with large scale which could provide high-speed access speed better than other access modes. As the supplement of 3G, it can be also used to solve the bottleneck problem of access network, and its market

prospect will be quietly good after it is used in civil purposes. Therefore, with further studies, many problems puzzling the Ad Hoc network will be solved finally, and the Ad Hoc network will be applied in more domains.

**References**

Cao, Sanfeng. (1996). Wireless Computer Networking and Technology. *Journal of Jiangxi Institute of Education.* No. 6.

Dong, Huomin, Li, Sen & Tian, Qing. (2000). Comparison and Analysis of the Wireless and Wire Network Solutions. *Application Research of Computers.* No. 9.

Fang, Xuming. (2003). The Current Research and Development of Mobile Ad Hoc Network. *Data Communications.* No. 4.

Jiang, Hai, He, Yongming & Cheng, Shixi. (2001). Research on Key Techniques of Mobile Ad Hoc Network. *The 7th Annual Symposium of ZTE Communication Technology.*

Ma, Chuanming, Xie, Xianzhong & Nie, Neng. (2003). The Connectivity of Mobile Ad Hoc Networks and Internet. *China Data Communications.* No. 9.

Wang, Qun & Li, Fujuan. (1999). Elementary Description of Wireless Local Area Network Technology. *Computer & Communications.* No. 10.

Table 1. Model of NS2 Simulator

| Node | Motion time | Motion speed | Motion direction |
|---|---|---|---|
| Node 0 | 0 | | |
| Node 1 | 1.5 s | 0.5 m/s | (500, 500) |
| Node 2 | 1.5 s | 1 m/s | (0, 0) |
| Node 3 | 1.5 s | 1 m/s | (0, 0) |
| Node 4 | 0 | | |

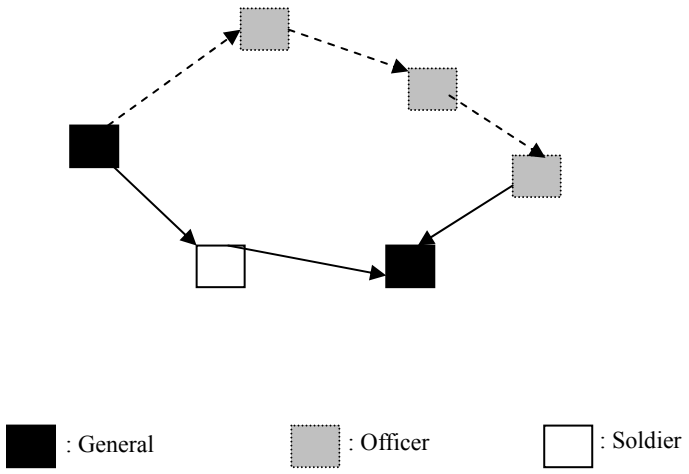


Figure 1. Purpose of SAR Routing Technology

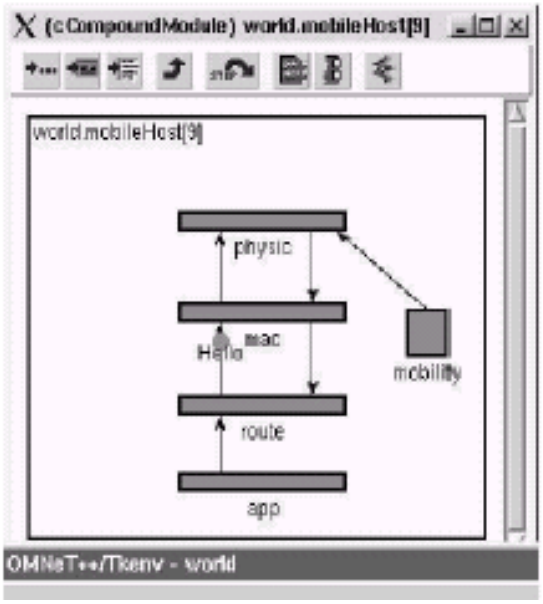


Figure 2. Relationship of Modules of Ad Hoc Simulator Nodes

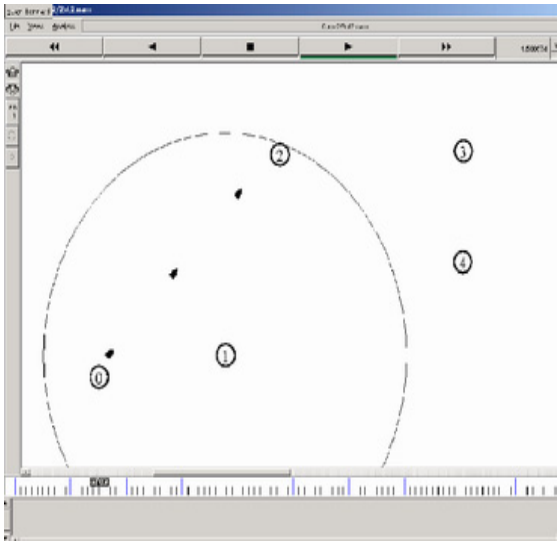


Figure 3. Topological Structure of the Network at 1.500574 s When Using NS2 Simulator

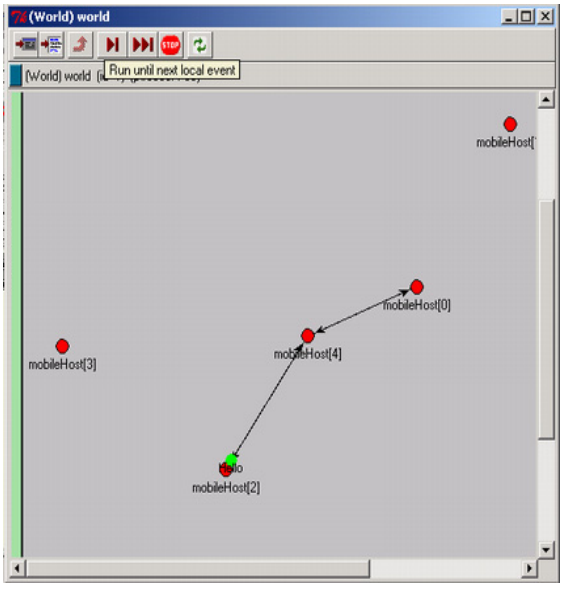


Figure 4. Topological Structure of the Network at 18.00 s When Using OMNet++ Simulator

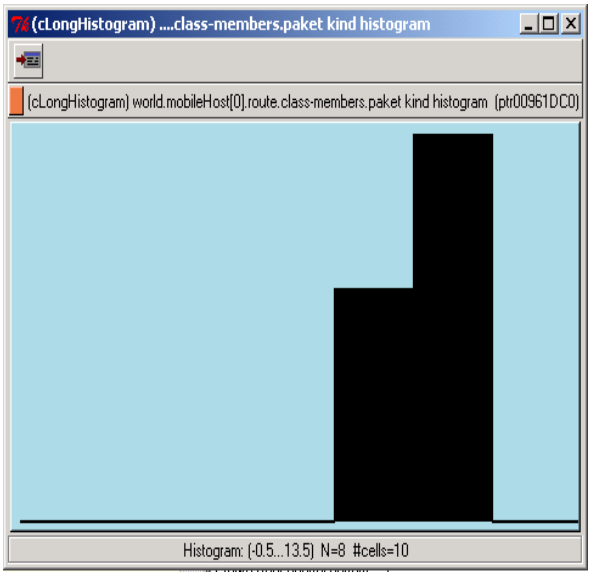


Figure 5. Packet Histogram of the Node 0 in the Simulation


ISSN 1913-8989 E-ISSN 1913-8997