doi:10.2498/cit.1000748

Using Network Processor to Establish Security Agent for AODV Routing Protocol

Chen Hongsong[1,2], Fu Zhongchuan[2], Wang Chengyao[1], Ji Zhenzhou[2],
Hu Mingzeng[2]

[1]Department of Computer Science, University of Science and Technology Beijing
[2]Department of Computer Science and Technology, Harbin Institute of Technology

Network processor (NP) is optimized to perform network tasks. It uses massive parallel processing architecture to achieve high performance. Ad hoc network is an exciting research aspect due to the characters of self-organization, dynamically topology and temporary network life. However, all the characters make the security problem more serious. Denial-of-Service (DoS) attack is the main puzzle in the security of Ad hoc network. A novel NP-based security scheme is proposed to combat the attack. Security agent is established by a hardware thread in NP. Agent can update itself at some interval by the trustworthiness of the neighbor nodes. Agent can trace the RREQ and RREP messages stream to aggregate the key information and analyze them by intrusion detection algorithm. NS2 simulator is expanded to validate the security scheme. Simulation results show that NP-based security scheme is effective to detect DoS attack.

Keywords: network processor, AODV routing protocol, security Agent, DoS attack, intrusion detection, performance evaluation.

1. Introduction

With the ever-increasing performance and flexibility requirements seen in today's networks, programmable network processors have been developed to meet the need. Network processor(NP) is a programmable device with architectural parallel features and special optimization for packet processing[1]. Most network processors use hardware multithreading computing model. Separate register files and contexts for separate threads ensure fast context switching. The multithreading parallel architectures fit to multi-task execution environment in network. Thus each thread is related to a task. New general programmable routers are designed by network processor, especially for security application.

Ad hoc networks are dynamic collections of self-organizing mobile nodes with links that are changing in an unpredictable way. They are characterized by a dynamic topology. Nodes can perform the roles of both hosts and routers with intrinsic mutual trust. In Ad hoc network, every node acts as router to form the network, security is very important to ad hoc networks. In wireless Ad hoc network, wireless nodes require process flexibility with low power consumption and high security, network processor is very fit to the need. So we use network processor to build the node of Ad hoc security scheme is designed by the network processor.

2. Related Research Work

There are two main approaches in current Ad hoc securing environments. The first is intrusion prevention measures, such as authentication and encryption. The second is intrusion detection and response approach [2].

Because cryptography-based prevention technique consumes much energy, it is invalid to internal attacks [3]. Intrusion detection and response are a necessity in MANET. We introduce them by the system architecture.

1) Zhang and Lee build on the completely distributed structure of wireless Ad hoc networks. Every node in the network partic-

ipates in the process of intrusion detection [4]. Each node is responsible for detecting intrusion locally and independently based on the data collected by itself. They use data on the node's physical movements and the corresponding change in its routing table as the trace data to build the anomaly detection model.

Because all the nodes run local detection engine that analyzes local data for anomalies, it is too expensive to detect some special attacks.

2) Hierarchical IDS architectures have been proposed for multi-layered [5], wireless Ad hoc networks. In a multilayered wireless Ad hoc network, cluster-head nodes centralize routing for the cluster and may support additional security mechanisms. The whole network is logically divided into several clusters, each of them consists of one special node as the cluster head and several normal nodes as the cluster members.

Because the cluster heads are the main communication and intrusion detection center, if the cluster heads have been attacked by malicious attackers, the network will be destroyed.

3) Oleg Kachirski proposes Multiple Sensors intrusion detection system for Ad hoc wireless networks based on mobile agent technology [6]. They introduce a multi-sensor intrusion detection system employing cooperative detection algorithm. A mobile agent implementation is chosen, to support such features of the IDS system as mobility of sensors, intelligent routing of intrusion data throughout the network and lightweight implementation.

Because of scarce computational and power resources in mobile nodes, multiple sensors and agent communication impose heavy pressure on Ad hoc network.

3. The Ad hoc On-Demand Distance Vector (AODV) Protocol

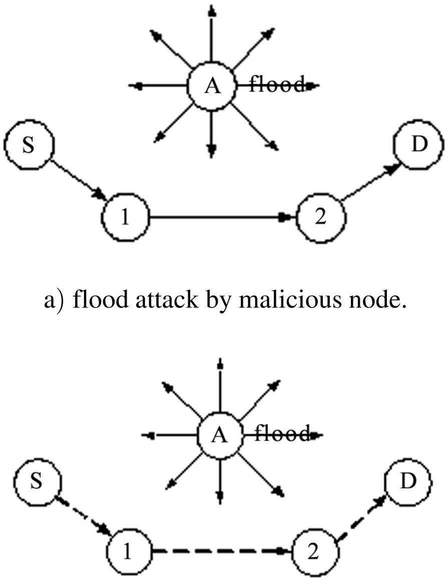
The Ad Hoc On-Demand Distance Vector (AODV) algorithm enables dynamic, self-starting, multi-hop routing between participating mobile nodes wishing to establish and maintain an Ad hoc network [7]. AODV allows mobile nodes to obtain routes quickly for new destinations and does not require nodes to maintain routes to destinations that are not in active communication. AODV is a reactive and stateless protocol that establishes routes only as desired by a source node using route request (RREQ) and route reply (RREP) messages. When a source node wants to send data packets to a destination node, but cannot find a route in its routing table, it broadcasts RREQ messages to its neighbors. Its neighbors then rebroadcast the RREQ message to their neighbors if they do not have a fresh enough route to the destination node. This process continues until the RREQ message reaches the destination node or an intermediate node that has a fresh enough route. After accepting a RREQ message, the destination or intermediate node updates its reverse route to the source node using the neighbor from which it has received the RREQ message. When the source or an intermediate node receives a RREP message, it updates its forward route to the destination node, using the neighbor from which it has received the RREP message. The source node, or an intermediate node, updates its routing table if it receives a RREP message.

4. Denial-of-Service Attack to AODV Protocol

A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. It can consume scarce resources or destroy network connection. These attacks do not necessarily damage data directly or permanently, but they intentionally compromise the availability of the resources [8]. They can consume much useful resource to disrupt network usability. DoS attacks in AODV protocol routing level can be classified into two categories by the type of message – RREQ flood attack and RREP route loop attack.

4.1. RREQ Flood Attack

The flood attack introduces unnecessary broadcast messages into the network to hinder normal operation of the network, the malicious node continually sends a mass of route requests to force the neighbors to process these packets and therefore consume batteries and network bandwidth. RREQ flood attack is shown in Figure 1.



a) flood attack by malicious node.

b) after RREQ flood attack.

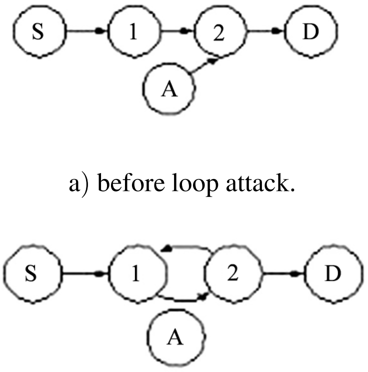
Fig. 1. Flooding attack caused by RREQ flood.

As shown in Figure 1, malicious node sends a mass of fake RREQ broadcast to flood the network. Other nodes process and response the flood RREQ, the flood makes great impact on the storage and communication resource of the nodes. It almost causes the network communication breakdown.

4.2. RREP Route Loop Attack

A routing loop is a path that goes through the same node more than once. Routing loops cause packets to be sent by the same nodes over and over again until the TTL-field in the packet is exhausted to zero. Routing loops can be used to create DoS, because they consume node resources in the loop. The destination node can also be isolated from the network, because only few packets reach their destination. Figure 2 shows that a route loop is formed between node 1 and node 2.

As Figure 2 shows, there are two intermediate nodes in a route from node S to node D. The attacker can form a route loop between node 1 and node 2, by pretending to be node 1 to forward a RREP message with increased RREP sequence. When node 2 receives the fake RREP message, it updates the next hop from node D to node 1. After updating the destination sequence number in the route table, these packets will be first sent to node 1, then node 2 and back to node 1 again. As a result, a route loop is formed between node 1 and node 2.



a) before loop attack.

b) after loop attack

(Node S: originating node; nodes 1 and 2: intermediate nodes; node D: destination node; node A: attack node).

Fig. 2. The attacker forms a loop between node 1 and node 2 by a fake RREP message.

5. NP-based Security Scheme in Ad hoc Network

Recently, main attention has been paid to the security processor design for wireless Ad hoc devices. However, there is a lack of research for combining security application and network processor in wireless communication. In this paper, we present the design of security agent by network processor to meet the security need of wireless Ad hoc network. Ad hoc networks are characterized by dynamic topology and the lack of fixed infrastructure. Ad hoc wireless networks allow people to set up computer networks and access information at any place and time. Nodes can perform the roles of both hosts and routers with intrinsic mutual trust. The nature of mobile computing environment makes it vulnerable to malicious attacks.

Traditionally, security processing has been achieved using software. However, due to the increasing demand for securing information, software solution may not be the best choice. The reason is that security algorithms are very time consuming and require powerful computational ability. Multithreading and

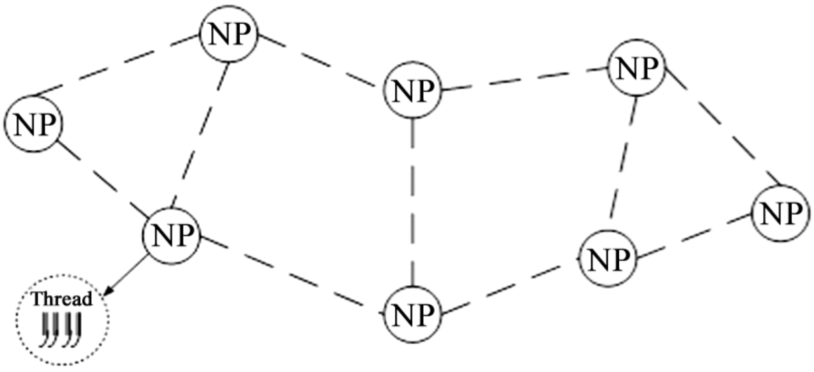


Fig. 3. NP-based distributed Wireless Ad hoc network.

programmable NP is used to establish mobile node in out security scheme. It can execute multi-task, such as routing tables management, packet classification and forwarding, security computation. Most of security processors existing in today's market are designed to function as security co-processors. Security co-processor is attached to network processor and invoked whenever the host processor decides that security processing is needed [9]. The approach moves the burden of security processing from the NP to the co-processor. The main limitation of this method is the need for a packet to traverse the memory many times. The communication between network processor and security co-processors brings long delay. This makes the network security performance depressed.

Therefore, finding new solutions that enhance security processing in Ad hoc network is essential. In fact, the security co-processor executes some types of algorithm for encryption and decryption. While in Ad hoc network, intrusion detection method is better than traditional encryption, especially for some types of DoS attacks, such as flooding attack. Because most network processors use hardware multithread architecture to fit multi-tasks in network environment, we use one of the threads as security agent to do security computing, while other threads do other network processing such as packet forwarding. So the advantage of the hardware multithread can be fully utilized without using security co-processor. This solution can save power consumption to meet the need of wireless network.

5.1. NP-based Intrusion Detection and Security Scheme

Lee's distributed IDS for Ad hoc network is the basic system model. The cost of intrusion detection increases with the number of nodes. Hierarchical IDS architecture is a model partitioned by node space location. Multiple Sensors intrusion detection system is a model partitioned by the functions of intrusion detection sensor. AODV routing protocol is an on-demand routing protocol, which initiates route discovery process when needed. As we use one thread of NP as security agent, and the thread owns dynamical lifetime, agent-based dynamic lifetime security scheme is proposed to improve the efficiency of intrusion detection. It is an intrusion detection model **firstly partitioned** by route existent lifetime. The number of IDS is equal to the number of AODV RREQ-RREP stream. The cost of intrusion detection decreases greatly.

The NP-based Ad hoc network architecture is shown in Figure 3.

As seen in Figure 3, multithreading NP is used to be a node of Ad hoc network. One thread of NP is used as security agent. In artificial intelligence context, *agent* is an entity that perceives its environment with sensors, it acts on its environment with effectors [10]. Such an agent can be a hardware multithread with sensors and effectors. The *agent* is certain kinds of artificial intelligence programs with user's goal.

The thread has three states: ready, waiting and running. The thread transforms its state by the NP resource utilization and computing environment. The thread state transition diagram is shown in Figure 4.

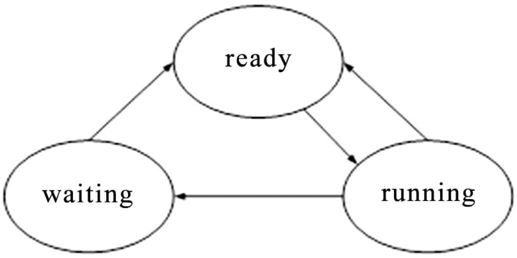


Fig. 4. Thread state transition diagram.

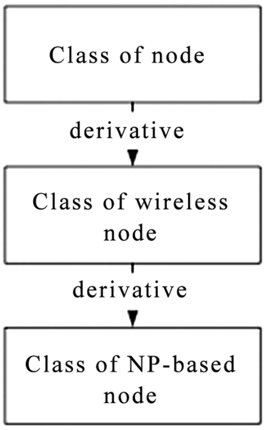


Fig. 5. Derivative relation of node class.

The following programming section shows the class definition of NP-based node:

```
Static class NP-node:
public wireless-node{
public: ---;
int thread-num; int thread-state;
int lifetime;
int thread-create();int thread-run();
int thread-wait();
int thread-destroy();};
```

The derivative relation of node class is shown in Figure 5.

The thread is created as security agent by the need of ADOV routing. Agent can change its state to reflect the state of the ADOV routing process. Security Agent is given dynamic life to avoid being attacked. Security Agent not only executes code and collects data, but also has multi-timed states. Security agent can create, execute, update and expire by the state of RREQ-RREP stream. When there is RREQ-RREP stream in network, there is a related security agent to monitor the stream by intrusion detection algorithm. After the RREQ-RREP stream disappears, the related security agent expires. Agent can update itself to improve trustworthiness and security. The timed finite state machine of security Agent is shown in Figure 6.

Seen from Figure 6, security protocol detects RREQ-RREP routing message periodically. If any RREQ-RREP stream is detected, security agent related to the stream is created to execute the intrusion detection algorithm. In fact, it is the hardware thread to execute the security code. After some interval, if the stream already exists in network, the current agent migrates to high trustworthiness neighbor node. Then another thread in the neighbor node will go on executing security code. So the intrusion detection algorithm is executed by many high trustworthiness neighbors in turns to distribute the cost of security computing and avoid the agent to be attacked. If there is no RREQ-RREP stream in network for some interval, the related agent expires by the stream. That is to

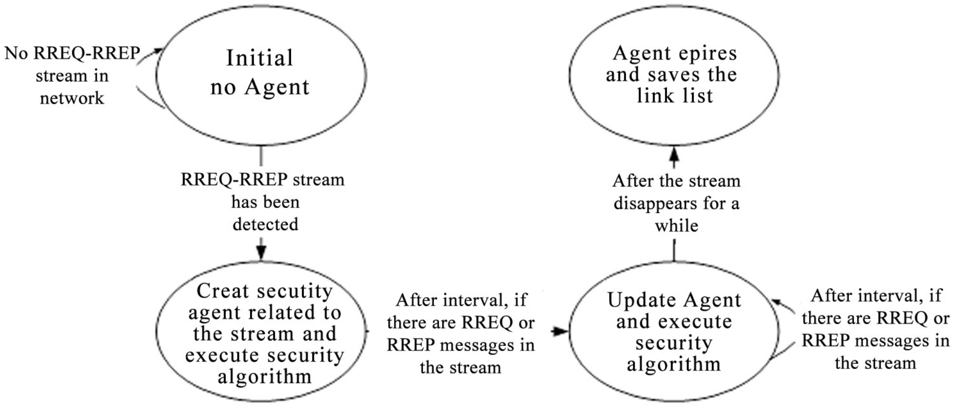

No RREQ-RREP stream in network
Initial no Agent
RREQ-RREP stream has been detected
Creat secutity agent related to the stream and execute security algorithm
After interval, if there are RREQ or RREP messages in the stream
Update Agent and execute security algorithm
After interval, if there are RREQ or RREP messages in the stream
After the stream disappears for a while
Agent epires and saves the link list

Fig. 6. The timed finite state machine of security Agent.

Security scheme Performance parameters	Completely distributed IDS security scheme	Agent based security scheme	SAODV Digital Signatures scheme
Packet format extension	No need	No need	Need
Key management	No need	No need	Need
Memory requirement	Medium	Medium	Medium
Computation complexity	Low	Low	High
Node Number to execute security scheme	All nodes	Part nodes	Part nodes
Security scheme lifetime	At all times	On-demand	At all times
Power dissipation	Medium	Low	High
Ability to detect DoS attack	Yes	Yes	No

Table 1. The comparison of the current security scheme in MANET.

say, the agent has dynamic lifetime to execute the security scheme. The comparison of current security scheme in MANET is listed in the Table 1.

We make the following assumptions in the security scheme.

1) Agent is a hardware thread that executes the security scheme. It can migrate between the high trustworthiness nodes.

2) Agent has the ability to access routing tables of nodes related to the stream. It should also have the capability of controlling node and intercepting RREQ and RREP related to the stream.

5.2. RREQ Flood Attack Detection and Response

In AODV routing process, when a source node needs a route to destination, it initiates a route discovery process. In route discovery, a route request can be uniquely identified by the RREQ ID, source sequence, source and destination route request address. In a route reply, reply message goes back to the source node over the shortest path. The routing information is stored in a trace link list shown in Table 2. It includes table head and table items. Every table head stands for a route discovery entrance. *RREQ-Count* stands for the number of RREQ broadcast in a period of time. It can be used to detect flood attack. Every table item stands for a message in the RREQ-RREP stream. Because the source and destination IP address in RREP message is reverse to the corresponding RREQ message, a Tag flag is used to distinguish them. If it is RREQ message, the Tag flag is 0; else it is RREP message, the Tag flag is 1. The construction of the trace link list is shown in Table 2.

The agent monitors the RREQ-RREP messages at real-time to fill in the trace link list. **In NS2 simulator, the security agent monitors the RREQ and RREP messages by calling rece( ) function. Once the RREQ messages are received, they will be processed by security agent**. The Agent exists with the stream. After the RREQ-RREP stream disappears for some interval, the Agent expires, but the link list already exists in the node. RREQ flood attack will be processed by the following algorithm shown in Table 3.

When the Agent hears a RREQ message, it firstly compares if the IP address in IP header of the RREQ message is equal to AODV source route address. If they are equal, it is a new RREQ-RREP stream, the key information of

rreq_src1	rreq_dst1	rreq_bid1	PREQCount1	source_seq1	dest_seq1	→	ipsrc1	ipdst1	Tag	...
rreq_src2	rreq_dst2	rreq_bid2	PREQCount2	source_seq2	dest_seq2	⟶				
---	---	---	---	---	---	⟶				
rreq_srcn	rreq_dstn	rreq_bidn	PREQCountN	source_seqN	dest_seqN	⟶				

Table 2. The construction of the trace link list.

```
1. Agent is created by a thread of NP.
   The value of RREQ ID trace table head and the count of RREQ is set to zero. //Initiate the trace table
2. RREQ messages are received by agent and some useful information are extracted to be analyzed.
3. if(source route address of RREQ==source IP address of the message) // Judge if it is a new RREQ request
     then {
       Source and destination address of RREQ, broadcast ID and source sequence number are stored in a row
   of the RREQ ID trace table head.
             RREQCount⇓RREQCount+1.    //Incrace the count of RREQ in an initial RREQ-RREP stream
               if (RREQCount> threshold in an interval) then
               {  RREQ flood is detected. //Judge the flood attack
                  The node that send the faked RREQ will be isolated from the network.
                  The node ID will be added to a blacklist . //Intrusion response
                 }
                  Else forward the RREQ normally //Normal route process
               }
     Else { agent adds the key information of the RREQ massage into the item of related link list.
              forward the RREQ normally. }
```

Table 3. RREQ flood intrusion detection and response algorithm.

the RREQ message is saved in the head of the link list to record the stream. If they are not equal, the Agent looks up the head of link list to validate if the related link list was built to the stream. If the related head of the link list is found, the Agent goes on to check the previous node to send the RREQ message. If the previous node is found, the Agent validates the data and directs consistency between the current RREQ message and the RREQ message received by previous node. The source sequence number of the current RREQ message should be equal to that of the RREQ message received by previous node. The hop count should be increased by 1. When all the above validation has passed, the Agent adds the key information of the RREQ message into the item of related link list, the RREQ is forwarded correctly. Otherwise fake RREQ attack is detected, the message is dropped; the node to send the RREQ is isolated and recorded into blacklist.

6. RREP Loop Attack Detection and Response

The biggest difference between the intrusion detection for RREQ and RREP is in that the former builds the link list, the latter checks and updates the link list.

As Table 4 shows, the Agent monitors the RREP at real-time to update the trace table, it detects the route loop attack by RREP route loop detection algorithm and drops the malicious RREP message.

When a RREP message is heard by Agent, it checks the head of link list to validate if the related link list was built to the RREQ-RREP stream. If it finds the head related to the stream, Agent goes on to find the corresponding RREQ item and the previous node. If the value of tag is more than 1, at the same time the source-destination IP address in RREP is equal

```
1. RREP messages are received by agent and some useful information are extracted to be analyzed.
2. RREP messages are grouped by their RREP source and destination address.
3. if (one source IP address of RREP message == destination IP address of previous RREP message &&its
   destination IP address of RREP == the source IP address of previous RREP message)
     then
       { RREP route loop is detected. //Route loop detection
       The malicious RREP message will be dropped.
       The node ID relating to the malicious RREP message will be added to the blacklist.
                                //Intrusion response
       }
     else { Update the Tag value in the related item of trace link list.
       forwarding the RREP normally. }
```

Table 4. RREP route loop detection and response algorithm.

to destination-source IP address in the previous RREP, the RREP loop attack is detected. When attacks are detected by agent, the RREP is dropped, the malicious node is recorded into blacklist.

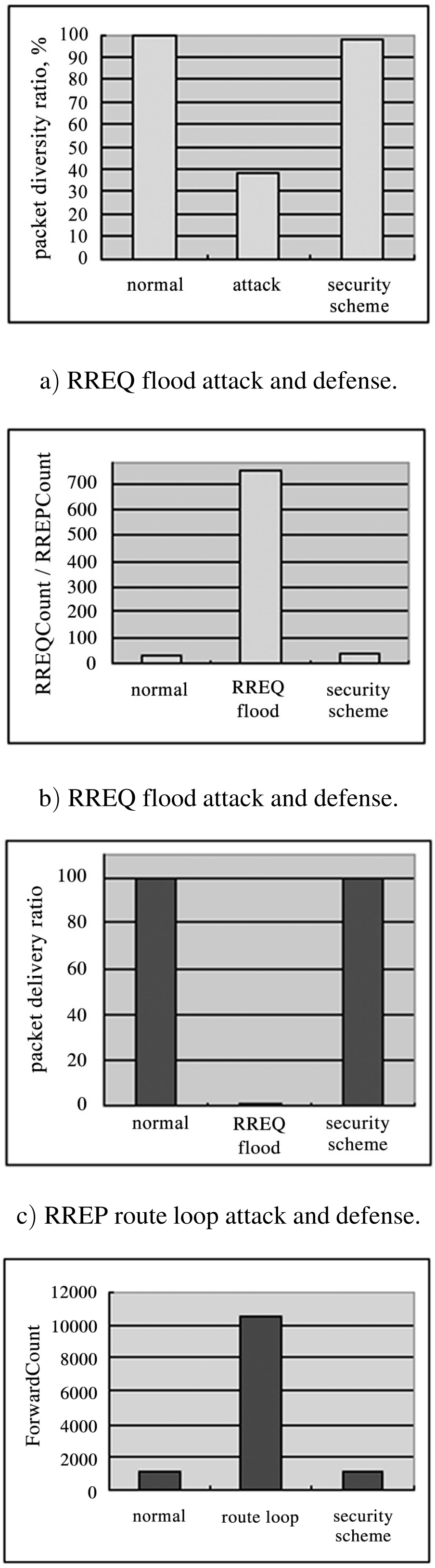
7. Performance Evaluation and Simulation Results

The measurements of the network performance are made by the NS2 [11]. In order to validate NP-based security scheme, we extend the node type to multithreading architecture, it is realized by node configure, we add multithreading description to the node architecture. Table 5 shows the parameters used in our experiments. Continuous bit rate (CBR) is used in our experiments. There are 20 nodes in the Ad hoc network. The simulation runs for 300 seconds. The field configuration is 1 000 m × 600m. The physical link bandwidth is 2 Mbps. The node architecture is multithreading.

Communication Type	CBR
Number of Nodes	20
Node architecture	multithreading
Simulation Area	1000m*600m
Simulation Time	300 seconds
Pause Time	2 seconds
Packet Rate	4packets/second
Number of Connections	5
Transmission Range	250m
Physical Link Bandwidth	2Mbps
Number of malicious nodes	1

Table 5. Simulation parameters.

DoS attacks in AODV protocol routing level can be classified into RREQ flood attack and RREP route loop attack. Performance evaluation to the two types of DoS attacks are shown in Figure 6.



a) RREQ flood attack and defense.

b) RREQ flood attack and defense.

c) RREP route loop attack and defense.

d) RREP route loop attack and defense.

Fig. 7. Performance evaluation of NP-based dynamic lifetime security scheme.

Figure 7 shows that the two types of DoS attacks have great effect on the performance, while NP-based security scheme can effectively detect the attacks and block the attackers. Seen from Figure 7a), packet delivery ratio in normal is 100%; under RREQ flood attack, the metric decreases to 47% while under security scheme, the malicious node is detected and isolated, the metric recovers to 98%, it is near to the normal level. Seen from Figure 7b), the ratio RREQCount/RREPCount in normal is 2848/86=33, the ratio value under attack increases to 250059/332=751, while the ratio value under NP-based security scheme decreases to 6208/159=39. Agent-NP security scheme can detect the RREQ flood attack on time, yet there is little influence at the beginning of attack.

In route loop attack, the packet delivery ratio greatly decreases from 100% to 1.1%, while the ratio value increases to 100% under NP-based security scheme as shown in Figure 7c). ForwardCount – the number of forwarded packet in normal is 1117, it greatly increases to 10491 in attack, while it decreases to 1143 in NP-based security scheme. As shown in Figure 7d), when the malicious RREP message is dropped, the route loop disappears, so the performance resumes near normal level. Simulation results show that the security scheme is most effective with the two types of DoS attacks.

To research the effect of number of nodes and packet rate on security scheme, we change the number of nodes and packet rate to analyse the result. The parameters can be easily changed in NS2 simulator.

When the number of nodes is increased to 40, packet delivery ratio under attack is 59%, it is more than the ratio in node number 20; while the metric increases to 96% in my security scheme. Since AODV is an on-demand routing protocol, it is sensitive to this metric, my security scheme is efficient to DoS attack.

When packet rate is increased to 8packets/second, the ratio RREQCount/RREPCount under attack is 391559/473=823, while the metric decreases to 8673/223=39 in my security scheme. It shows that the scheme is efficient.

8. Conclusion

In this paper, DoS attacks for AODV routing protocol are classified and analyzed. A novel intrusion detection scheme based on NP is proposed to combat the attacks. It is an intrusion detection and response model **firstly partitioned** by the route existent lifetime. A hardware thread in NP acts as security agent to execute intrusion detection and response. The security Agent can change its state with the AODV routing process to save energy. The Agent can update itself to a higher trustworthiness neighbor to keep the high trustworthiness of network. The number of Agents is equal to that of RREQ-RREP stream. The Agent can build and update link list to trace the RREQ-RREP message stream.

Simulation results show that the attacks have great effect on the system performance. NP-based dynamic lifetime security scheme can efficiently detect the attacks and isolate the malicious node to make the network security performance metric **recover to normal** quickly. In the future, **Intel IXP 425 Network Processor will be used** as process core to establish Security Association in MANET. The research about the attack and security scheme for AODV protocol is meaningful to Ad hoc network security and future application.

Acknowledgments: The research has been supported by the National Natural Science Foundation of China (Grant No. 60475012) and National Defense Foundation of China (Grant No. 413460303). The authors wish to thank the anonymous reviewers for their detailed reviews and **many constructive suggestions** which have improved the paper significantly.

References

[1] BJÖRN LILJEQVIST, *Visions and Facts–A Survey of Network Processors*, [Master's Thesis], 2003.

[2] L. ZHOU AND Z. J. HAAS, Securing ad hoc networks, *Journal of IEEE Networks*, 1999, 13(6): pp. 24–30.

[3] J. P. HUBAUX, L. BUTTYAN AND S. CAPKUN, The quest for security in mobile ad hoc networks, *In Proc. ACM MOBICOM*, 2001.

[4] Y. ZHANG AND W. LEE, Intrusion Detection in Wireless Ad Hoc Networks, *In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom 2000)*, August, 2000, pp. 275–283.

[5] HONGMEI DENG, QING-AN ZENG AND DHARMA P. AGRAWAL, SVM-based Intrusion Detection System for Wireless Ad Hoc Networks, *Proceedings of the IEEE Vehicular Technology Conference (VTC'03)*, Orlando, October 6–9, 2003.

[6] OLEG KACHIRSKI, RATAN GUHA, Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks, *Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03)*, Vol. 02, February 2003, pp. 57–65.

[7] PERKINS, E. S. DAS, *Ad hoc on-demand distance vector(AODV) routing*, Internet Draft, draft-ietf-manet-aodv-13.txt (February 2003).

[8] KARLOF AND D. WAGNER, Secure routing in wireless sensor networks: Attacks and countermeasures. *In First IEEE International Workshop on Sensor Network Protocols and Applications*, 2003, pp. 1–15.

[9] KHAN, ESAM, Network Processors for Communication Security: A Review, *IEEE Pacific RIM Conference on Communications, Computers and Signal Processing*, 2003, pp. 173–176.

[10] WONG S. K. JOHNNY AND MIKLER R. ARMIN, Intelligent Mobile Agents in Large Distributed Systems, *In the Journal of systems and software*, 1999, 47, pp. 75–87.

[11] `http://www.isi.edu/nsnam/ns`

Received: September, 2005
Revised: March, 2006
Accepted: May, 2006

Contact addresses:

Chen Hongsong
Department of Computer Science
University of Science and Technology
Beijing, 100 083

Fu Zhongchuan
Department of Computer Science and Technology
Harbin Institute of Technology
Beijing, 150 001

Wang Chengyao
Department of Computer Science
University of Science and Technology
Beijing, 100 083

Ji Zhenzhou
Department of Computer Science and Technology
Harbin Institute of Technology
Beijing, 150 001

Hu Mingzeng
Department of Computer Science and Technology
Harbin Institute of Technology
Beijing, 150 001

CHEN HONGSONG was born in 1977. At the moment he works at the University of Science and Technology Beijing. He received his Ph.D. degree in computer science from Harbin Institute of Technology in April 2006. His research interests include high performance and low power network processor design, and ad hoc network security routing protocol.

FU ZHONGCHUAN was born in 1970. He is a Ph.D. candidate in the Department of Computer Science and Technology of Harbin Institute of Technology. His research interest is high performance processor design.

WANG CHENGYAO was born in 1966. He works as a professor at the University of Science and Technology Beijing. His current research field includes AI, soft test.

JI ZHENZHOU was born in 1965. He works as a professor in the Harbin Institute of Technology. His current research field includes parallel processes and Ad hoc/sensor net routing protocol research.

HU MINGZENG was born in 1935. He is a professor in the Harbin Institute of Technology. His current research field includes parallel processes and network security.