Asian Journal of Information Technology, 5 (1) : 54-60 , 2006

A Novel Security Agent Scheme for Aodv Routing Protocol Based on Thread State Transition

[1,2]Chen Hongsong, [1,2]Ji Zhenzhou and [1,2]Hu Mingzeng
[1]Department of Computer Science and Technology Harbin Institute of Technology, 150001
[2]National Computer Information Content Security Key Laboratory, Harbin 150001, China

Abstract: Ad HOC network is vulnerable to attacks due to the characters of self-organization dynamically changing topology and temporary network life. Black hole attack is the main puzzle in the security of Ad HOC network. There are not satisfied solutions to solve the problem. A novel security agent scheme is proposed to combat the attack in AODV routing protocol. Network Processor (NP) uses parallel multithreading architecture to achieve high performance. Security agent is established by a hardware thread in NP. Agent has dynamic lifetime as the thread state transition. Agent can migrate to higher trustworthiness neighbor nodes. It appears in right time and space in our security scheme. The number of Agent is equal to the number of AODV routing stream. Agent can trace the key information of AODV routing stream and analyze them by intrusion detection algorithm. Simulation results show that performance metric decreases from about 2.2 KByte/s to nearly 0 KByte/s under Black hole attack, however it recovers to about 2.2 KByte/s in our security scheme.

Key words: AODV routing protocol, security agent, multithreading, black hole attack, intrusion detection, performance evaluation

INTRODUCTION

With the ever-increasing performance and flexibility requirements in network, programmable network processor has been developed to meet the need. Network processor (NP) is programmable device with architectural parallel features and special circuit for packet processing[1]. Thread-Level Parallelism exists between different execution programs. Most network processors use hardware multithreading model. Separate register files and contexts for separate threads ensure fast context switch. The multithreading parallel architectures fit to multi-task network environment. New general programmable routers can be designed by network processor, especially for security application.

Ad hoc networks are dynamic collections of self-organizing mobile nodes. They are characterized by dynamic topology and lack of any fixed infrastructure. In Ad HOC network, Nodes perform the roles both hosts and routers. The nodes require high security and low power dissipation, network processor is very fit to the need. So we use network processor to be the core of the node, security scheme is implemented by the thread of network processor.

RELATED RESEARCH WORK

There are two main approaches in current Ad HOC security mechanism. The first approach is intrusion prevention technology, such as authentication and encryption. The second approach is intrusion detection and response[2].

Because cryptography-based security mechanism consumes much energy and it is invalid to internal attacks[3], intrusion detection and response is very important in Ad HOC security. We introduce them by system architecture of security model.

- Zhang and Lee propose completely distributed structure of wireless Ad HOC networks. Every node in the network participates in the process of intrusion detection[4]. Each node is responsible for detecting intrusion locally and independently. They use data change in routing table as the trace data to build anomaly detection model. Because all the nodes run detection engine, it is too expensive to detect attacks.
- Hierarchical IDS architecture[5] has been proposed for multi-layer Ad-HOC networks. In a multi-layer wireless ad-hoc network, the whole network is logically divided into several clusters, each of them consists one special node as the cluster head and several normal nodes as the cluster members. Because cluster heads are communication and detection center, if cluster heads have been attacked, the network will be destroyed.
- Oleg Kachirski proposes Multiple Sensors intrusion detection system for Ad HOC wireless networks based on mobile agent technology[6]. They

Corresponding Author: Chen Hongsong, No.92, West Da-zhi Street, Harbin, Heilongjiang Province, China P.O. No. 320 Postalcode: 150001

introduce amulti-sensor intrusion detection system employing cooperative detection algorithm. It employs several sensor types that perform specific certain functions, such as: Network monitoring Host monitoring Decision-making Action. Because of scarce computational and power resources in mobile nodes, multiple sensors and agent communication bring pressure to Ad HOC network.

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 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 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 messages reach 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. When source or intermediate node receives a RREP message, it updates its routing table to the destination node.

BLACK HOLE ATTACK TO AODV PROTOCOL

In black hole attack, all network traffics are redirected to a specific node which does not exist at all[8]. Because traffics disappear into the special node as the matter disappears into Black hole in universe. So the specific node is named as Black hole. Black hole attacks in AODV protocol routing level can be classified into two categories-RREQ Black hole attack and RREP Black hole attack.

Black hole attack caused by RREQ: An attacker can fake RREQ messages to form black hole attack. In RREQ Black hole attack, the attacker pretends to rebroadcast a RREQ message with a non-existent node address. Other nodes will update their route to pass by the non-existent node to the destination node. As a result, the normal route will be broken down. The attacker can generate Black hole attack by faked RREQ message as follows:

- Set the type field to RREQ (1);
- Set the originator IP address to the originating node's IP address;

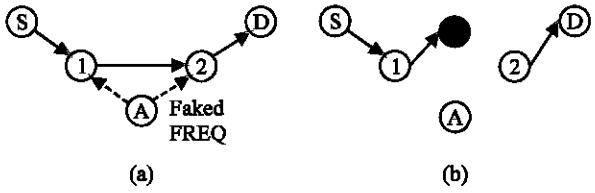

Fig. 1: Black hole is formed by Faked RREQ

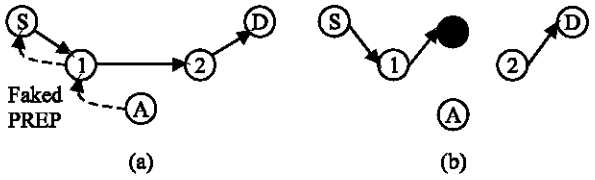

Fig. 2: Black hole is formed by Faked RREP

- Set the destination IP address to the destination node's IP address;
- Set the source IP address (in the IP header) to a non-existent IP address (Black hole);
- Increase the source sequence number by at least one, or decrease the hop count to 1.

The attacker forms a Black hole attack between the source node and the destination node by faked RREQ message. It is shown in Fig. 1.

Black hole attack caused by RREP: The attacker may generate a RREP message to form Black hole as follows:

- Set the type field to RREP (2);
- Set the hop count field to 1;
- Set the originator IP address as the originating node of the route and the destination IP address as the destination node of the route;
- Increase the destination sequence number by at least one;
- Set the source IP address (in the IP header) to a non-existent IP address(Black hole).

The attacker unicasts the faked RREP message to the originating node. When originating node receives the faked RREP message, it will update its route to destination node through the non-existent node. Then RREP Black hole is formed. It is shown as Fig. 2.

SECURITY AGENT SCHEME BASED ON THREAD STATE TRANSITION

Ad HOC wireless networks allow people to set up networks and access information at any place and time. They are characterized by dynamic topology and lack of

fixed infrastructure. The nature of mobile computing environment makes it vulnerable to malicious attacks. Researchers have paid attention to the design of security processors for wireless Ad HOC network. However, there is lack of research on combining Ad HOC network security and network processor application. In this paper, we propose the design of Ad HOC security agent by using the thread of network processor.

Traditionally, security process has been achieved by software solution. However, due to the speed need for network security, software solution is not the best choice. The reason is that security algorithms are very time consuming. Most of security processors are designed to 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 packet to traverse the memory many times. The communication between network processor and security so-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, security co-processor executes some types of encryption and decryption algorithm. While in Ad HOC network, intrusion detection method is better than traditional encryption. Multithreading and programmable NP is used to establish mobile node in Ad HOC network. It can execute multi-task, such as security computation routing tables update and packet forwarding. As most network processors use hardware multithread architecture to process multi-tasks in network environment, we use one of the threads as a security agent to do security task, while other threads do other network process tasks. So the advantage of the hardware multithread can be fully utilized while do not use security co-processor. This solution can save power consumption to meet the need of wireless Ad HOC network.

Intrusion detection and response based on thread state transition: Lee's distributed IDS for Ad HOC network is a basic system model. The cost of intrusion detection increases with the number of nodes. Hierarchical IDS architecture is a model partitioned by node physical location. Multiple Sensors intrusion detection system is a model partitioned by the function of intrusion detection sensors. AODV routing protocol is an on-demand routing protocol, which initiates route discovery process only as needed. We use one thread of NP as security agent, thread owns dynamical lifetime, agent-based dynamic lifetime security scheme is proposed. It is an intrusion

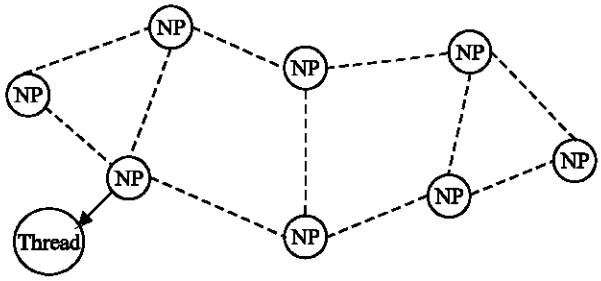

Fig. 3: New Wireless Ad HOC network architecture

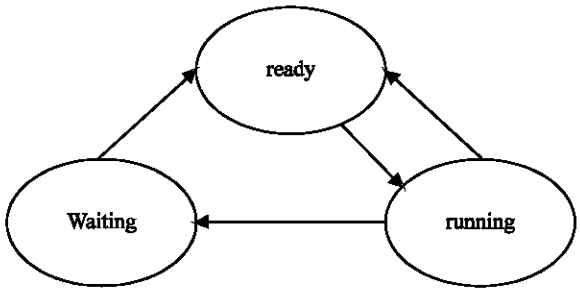

Fig. 4: Thread state transition diagram

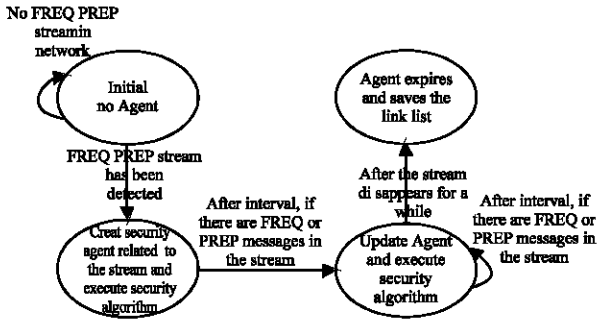

Fig. 5: Timed finite state machine of security Agent

detection model firstly partitioned by the route existent lifetime. The number of IDS is equal to the number of AODV RREQ-RREP stream. The cost of intrusion detection greatly decreases. The new Ad HOC network architecture is shown in Fig. 3.

As seen in Fig. 1, multithreading NP is used to be the process core of Ad HOC network node. One thread of NP is used to be security agent. In artificial intelligence aspect, *agent* is an entity that perceives its environment with sensors and acts on its environment with effectors[10]. The agent is certain kinds of artificial intelligence programs with user's goal. So a hardware multithread can become security agent with sensors and effectors. Thread has three states which are ready waiting and running states. Thread transforms its state by need of computing

Table 1: The construction of trace link list

rreq_srcl	rreq_dst1	rreq_bid1	RREQCount1	source_seq1	dest_seq1	iprc1 →	ipdst1	Tag	---
rreq_src2	rreq_dst2	rreq_bid2	RREQCount2	source_seq2	dest_seq2	→			
---	---	---	---	---	---	→			
rreq_srcn	rreq_dstn	rreq_bidn	RREQCountN	source_seqN	dest_seqN	→			

Table 2: RREQ Black hole intrusion detection and response algorithm

1. Agent is created by a thread of NP.
   RREQ ID trace table head and the count of RREQ is set to zero.
2. RREQ messages are received by agent and the key information is 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.}
   Else if (validate the head of link list to the stream was built)
   If(the previous node to send the RREQ message is found)
   If(The source sequence number of the current RREQ message== the RREQ message received by previous node ***&&*** The hop count increased by 1)
   {agent adds the key information of RREQ massage into the item of related link list;
   the RREQ is forwarded correctly; }
   Else { Black hole attack is detected;
   The node that send the faked RREQ will be isolated from the network;
   The node ID will be added to a blacklist;}
   Else { Black hole attack is detected;}
   Else { Black hole attack is detected;}

environment. The thread state transition diagram is shown in Fig. 4.

Security agent is created by thread in need of ADOV routing process. Security Agent not only executes code collects data,but also has multi-states to fit the need of AODV routing. Agent can change its state to reflect the state of the ADOV routing process. Security Agent is given dynamic life to avoid itself to be attacked. Security agent can create execute update and expire by the state transition of RREQ-RREP stream. When there is no RREQ-RREP stream in initial state, there is no security agent. When RREQ-RREP stream appears, there is a related security agent is created by thread to monitor the stream. Agent can dynamically migrate to higher trustworthiness neighbor rnode. After the RREQ-RREP stream disappears, the related security agent expires. The timed finite state machine of security Agent is shown in Fig. 5.

Seen from Fig. 5, security protocol detects the RREQ-RREP routing message periodically. If any RREQ-RREP stream is detected, security agent is created by a thread in NP to execute security algorithm. In fact, it is the hardware thread to execute the security agent code. After some interval, if the stream already exists in network, the current agent migrates to higher trustworthiness neighbor node. The packet forward rate is greater, the trustworthiness of the neighbor node is higher. Then another thread in the neighbor node will go on to execute the security agent code. So intrusion detection algorithm is executed by many high trustworthiness neighbors by turns. This scheme can distribute the cost of security computing and avoid the agent to be attacked. If there is no RREQ-RREP stream for some interval, the related agent expires, the thread state is waiting. That is to say, the agent has dynamic lifetime to execute the security scheme. We make the following assumptions in the security scheme.

- A hardware thread of NP executes security Agent code. Agent can migrate between the high trustworthiness nodes.
- Agent can access routing table entries of the nodes. It also has the capability to issue routing control message to isolate some special node.

RREQ Black hole detection and response algorithm: In AODV routing mechanism, 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 the source and destination route request address. In route reply, reply messages go back to source node by the shortest path. We design a trace link list to store routing information stream. It includes table head and table items. Every head stands for a route discovery entrance. Every item stands for the key message in the RREQ-RREP stream. As the source and destination IP address in RREP message is reverse to the RREQ message in the routing path, so Tag flag is used to distinguish them. If it is RREQ message, the Tag flag is 0;else it is RREP message, then the Tag flag is 1. The construction of trace link list (Table 1).

The agent monitors the RREQ-RREP messages at real-time to fill in the trace link list. Agent exists with the state of stream, after the RREQ-RREP stream disappears for some interval, the Agent expires, but the link list

Table 3: RREP Black hole intrusion detection and response algorithm

1. RREP messages are received by agent and the key information is extracted to be analyzed.
2. RREP messages are grouped by their RREP source and destination address.

If (the related RREQ Item is found)
if (The destination sequence number of the current RREP message==that of RREP message received by previous node && The hop count is increased by 1)
then
{ Update the Tag value in the related item of trace link list.
forwarding the RREP normally.
}
else { RREP Black hole is detected;
The malicious RREP message will be dropped;
The node ID relating to the malicious RREP message will be recorded to the blacklist;}
else { RREP Black hole is detected;}

already exists in the node. RREQ Black hole attack will be detected by the following algorithm (Table 2).

When agent hears a RREQ message, it firstly compares Ip address of the RREQ message with AODV source route address. If they are equal, it is a new RREQ-RREP stream, the key information of RREQ message is saved in the head of link list to record the stream. If they are not equal, agent looks up the head of link list to validate if related link list was built to the stream. If the related head of link list is found, agent goes on to check the previous node to send the RREQ message. If the previous node is found, agent validates data consistency between the current RREQ message and the RREQ message received by previous node. The source sequence number of current RREQ message should be equal to that of the RREQ message received by previous node. The hop count should be increased by 1.If all these validation pass, agent adds the key information of the RREQ massage into the item of link list, the RREQ is forwarded correctly. Otherwise Faked RREQ Black hole attack is detected the message is dropped ;the node to send the RREQ is isolated and recorded into blacklist.

RREP Black hole attack detection and response algorithm: The most difference between intrusion detection for RREQ and RREP is that the former builds the link list, while the latter checks and updates the link list.

The agent monitors RREP messages at real-time to update the trace table, it detects RREP black hole attack by intrusion detection algorithm (Table 3).

If it finds the head related to the stream, Agent goes on to look up the related RREQ item and the previous node to send the RREP message. If the previous node to send the RREP is destination node, destination sequence is saved in the item of link list head. If the previous node is intermediate node, Agent validates data consistency between current RREP message and the RREP message received by previous node. The destination sequence number should be equal. The hop count should be increased by 1. After all validations pass, agent updates the Tag value to 1. If any detection rule is not passed, Black hole attacks are detected, the malicious RREP message is dropped, the malicious node is isolated and the node ID is recorded to the blacklist.

PERFORMANCE EVALUATION AND SIMULATION RESULTS

The measurements of the network performance are made by ns2[11].In order to validate the security scheme, we extend the node type to parallel multithreading architecture, it is realized by node conFig.. Table 4 shows the simulation parameters configuration. Continuous bit rate (CBR) is used in our experiments. There are 20 nodes in the Ad HOC network. The simulation runs for 100 seconds. The simulation area is 1000*600m.The physical link bandwidth is 2 Mbps. The node architecture is parallel multithreading.

Black hole attacks in AODV routing protocol can be classified into RREQ Black hole attack and RREP Black hole attack. Performance evaluations to two types of Black hole attack are described in the following. Packet transmission speed between node 4 and node 5 is used to evaluate the security scheme under the two types of Black hole attacks Fig. 6.

Seen from Fig. 6, Black hole caused by RREQ has great effect on the traffic between node 4 and node 5.Packet transmission speed decreases from about 2.2KByte/s to 0KByte/s under RREQ Black hole attack. While in our security scheme, agent can detect the attacker by security algorithm. As security agent finds

Table 4: Simulation parameters

Communication Type	CBR
Number of Nodes	20
Node architecture	multithreading
Simulation Area	1000m*600m
Simulation Time	100 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

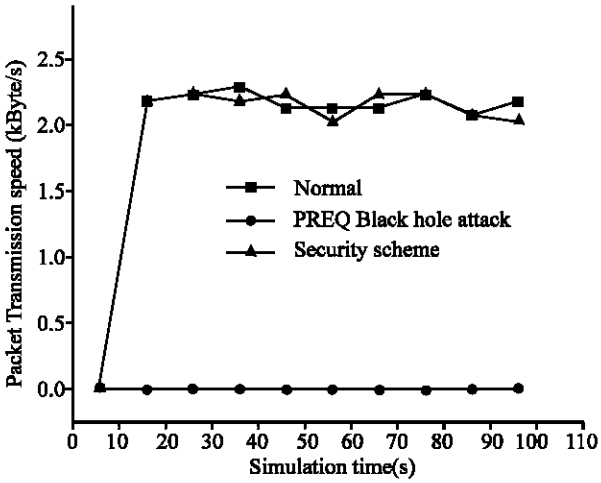

Fig. 6: Packet Transmission speed between node 4 and node 5

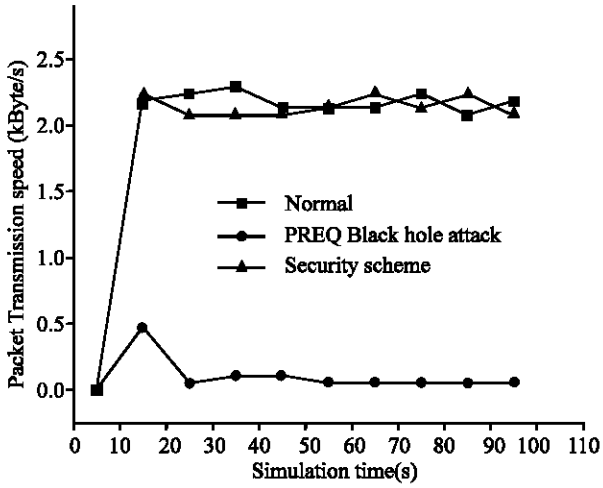

Fig.7: Packet Transmission speed between node 4 and node 5

that the malicious RREQ source sequence number is greater than the RREQ source sequence number in the trace table head, the malicious RREQ messages are dropped; malicious node is isolated and recorded to blacklist. The performance metric recovers to normal level.

Performance evaluation for RREP black hole attack and security scheme Fig. 7. Packet transmission speed between node 4 and node 5 is used to evaluate the performance of the security scheme.

Seen from Fig. 7, Black hole caused by RREP has great effect on the traffic between node 4 and node5. Packet transmission speed decreases from about 2.2KByte/s to almost 0 KByte/s under RREP Black hole attack. While in our security scheme, agent can not find the RREQ item related to RREP. Malicious RREP destination sequence number is greater than the RREP source sequence number in the trace table head. So the malicious RREP messages are dropped, the malicious node is isolated from the network and recorded into blacklist. The performance metric recovers to normal level.

Simulation result shows that the two types of Black attacks have great effect on network performance, while performance metrics recover to normal under our security scheme.

CONCLUSION

As wireless Ad HOC network is vulnerable to all kinds of attacks, security issues become a central concern. But there is not satisfied solution on Ad HOC network security. In this paper, a novel security scheme based on NP thread state transition is proposed to combat attacks. The main contributions in this paper are summarized into the following two points.

- We present a novel security agent scheme based on hardware thread in NP. Since thread has finite states, security agent may have timed finite states to meet the need of Ad HOC network security. It is an intrusion detection and response model firstly partitioned by route existent lifetime. The security Agent can dynamically change its state to implement security scheme and save energy. Agent can migrate to a higher trustworthiness neighbor node to avoid attacks. Security agent appears in right time and space in out security scheme. The number of Agent is equal to the number of RREQ-RREP stream, but not the number of nodes. Agent can build and update link list to trace RREQ-RREP message stream. It executes the intrusion detection and response algorithm based on the trace link list.
- To validate the security scheme, the node configuration of multithreading architecture is added into NS2 simulator. Black hole attacks for AODV routing protocol are used to test and analyze the efficiency of our security scheme. Simulation results show that Black hole attacks have great effect on network performance. Our security scheme can efficiently detect and block the attacks to make network performance recover to normal level quickly. The research about the attack and security scheme for AODV protocol is meaningful to Ad HOC network security and application in future.

ACKNOWLEDGEMENTS

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).

REFERENCES

1. BJÖRN LILJEQVIST, 2003. Visions and Facts-A Survey of Network Processors. Master's Thesis.
2. Zhou, L. and Z.J. Haas, 1999. Securing Ad HOC networks. J. IEEE Networks, 13: 24-30.
3. HuBaux, J.P., L. Buttyan and S. Capkun, 2001. The quest for security in mobile Ad HOC networks. In Proc. ACM MOBICOM.
4. Zhang, Y. and W. Lee, 2000. Intrusion Detection in Wireless Ad HOC Networks. In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom 2000), pp: 275-283.
5. Hongmei, D., Q.A. Zeng and D.P. Agrawal, 2003. SVM-based Intrusion Detection System for Wireless Ad HOC Networks. Proceedings of the IEEE Vehicular Technology Conference (VTC'03), Orlando, pp: 6-9.
6. Oleg, K. and G. Ratan, 2003. Effective Intrusion Detection Using Multiple Sensors in Wireless Ad HOC Networks. Proceedings of the 36th Hawaii Intl. Conference on Sys. Sci. (HICSS'03), 2: 57-65.
7. Perkins, E.S.D, 2003. Ad HOC on-demand distance vector(AODV) routing, Internet Draft, draft-ietf-manet-aodv-13.txt.
8. Karlof and D. Wagner, 2003. Secure routing in wireless sensor networks: Attacks and countermeasures. In First IEEE Intl. Workshop on Sensor Network Protocols and Applications, pp: 1-15.
9. Khan, E, 2003. Network Processors for Communication Security: A Review. IEEE Pacific RIM Conference on Commun., Computers and Signal Processing, pp: 173-176.
10. Wong, S., K. Johnny and R.A. Mikler, 1999. Intelligent Mobile Agents in Large Distributed Systems. In the J. sys. software, 47: 75-87.
11. http://www.isi.edu/nsnam/ns