Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 10, October 2015, pg.435 – 442

RESEARCH ARTICLE

Performance Evaluation of Various Quality of Service (QoS) Parameters of a Wireless Sensor Network under Black hole, SYN Flooding and Wormhole Attacks

Jatinder Singh
Research Scholar, Punjab, India
jsidhu88@hotmail.com

Abstract: ***Wireless Sensor Networks are used widely in numerous fields for countless applications such as pollution check, soil erosion, military applications etc. WSN include sensing + processing + storage + transmission. It has sensor nodes connected wirelessly deployed over an area or a person according to the requirement. It collects the information and sends it to the base station and server for analysis using radio frequency transmission at the real time. DoS attacks are such attacks which prevent the legitimate user from accessing the network or resources. Such attacks include blackhole attack, wormhole attack, ddos attack etc. Attack can be possible on the sensory nodes, routing path of the data .These attacks could change the data collected or even prevent the data from reaching the destination. This could lead to the incomplete or falsified data at the server which further results in a wrong interpretation of the crucial information regarding the specific area, person or environmental conditions etc. This is a paper about WSN under Black hole, Wormhole and SYN Flooding attacks. This paper shall provide a comparative analysis of the above mentioned attacks using Packet delivery ratio, Average Energy and Packet drop parameters.***

Keywords-Wireless Sensor Networks (WSN); Denial of Service Attack (DoS); Distributed Denial of Service Attack (DDoS); Packet Delivery Ratio (PDR).

I. INTRODUCTION

WSN is a wireless network of sensors deployed over an area or person to collect specific information and transmit it to the base station. WSN is a rapidly growing area of research and commercial development. They are very useful for military, environmental, and scientific applications to name a few. WSN comprises of nodes which require the battery power to operate. Generally the battery is required for communication [1].the battery power is limited so is the life of a WSN node. The various strategies have been formulated or under development which would reduce the energy consumption and increase the life of the WSN nodes which eventually make the commercial WSN more profitable. Some strategies are the use of the sleep and wait protocols.

II. BACKGROUND

WSNs architecture and characteristics

There are significant differences between WSNs and classical networks. The power is the main constraint in wsn networks because it determine the lifetime of a network. It is a major drawback because of the cost of replacing the battery especially in sensible environments. The architecture of a WSN may be viewed, according to [2], as follows:

1. *Infrastructure*: Consists of the sensors and their current deployment status.
2. *Network Protocols*: They are responsible for creating paths and accomplishing communication between the sensors, the base station and the observer/server.
3. *Application/Observer*: Interests in the phenomenon are queries from the observer(s). These queries could be static (the sensors are pre-programmed to report data according to a specific pattern) or dynamic. According to

the structure of nodes, we have two main architectures which influence significantly routing protocols [3]: in flat networks, each node typically plays the same role and sensor nodes topology of a WSN can be seen according to the mobility of nodes as static, mobile and collaborate together to perform the sensing task. In a hierarchical or cluster-based architecture, higher energy nodes (cluster-heads) can be used to process and send information while low energy nodes can be used to perform the sensing in the proximity of the target.

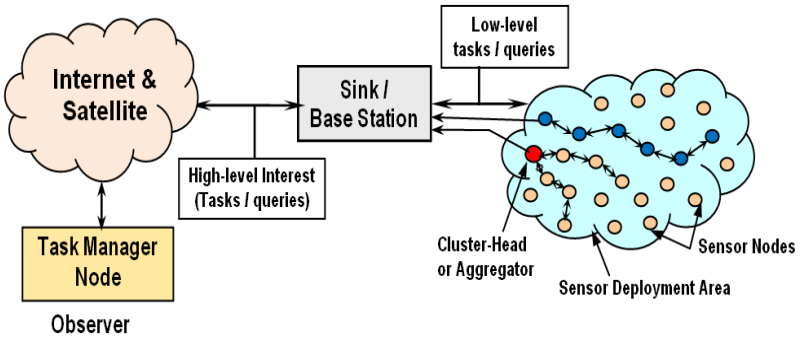

Fig. 1: WSN Architecture Overview [4]

III. WORMHOLE ATTACK

Wormhole attack is one of the Denial of- Service attacks effective on the network layer, that can affect network routing, data aggregation and location based wireless security. [5] In a typical wormhole attack, the attacker receives packets at one point in the network, forwards them through a wireless or wired link with much less latency than the default links used by the network, and then relays them to another location in the network.[6]

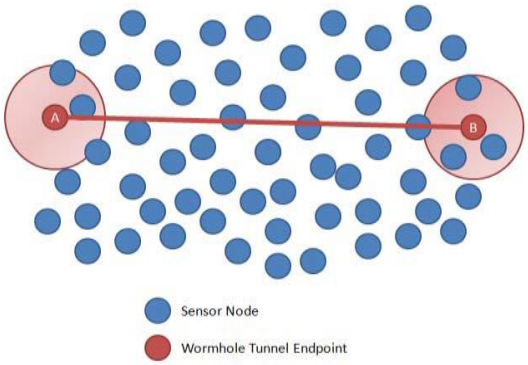

Fig 2: Illustration Wormhole Attack [7]

Fig 2 consist of large number of wireless sensor nodes with nodes A and B which act as wormhole nodes placed at the extreme ends transmitting data between each other with just one hop. They have illusion that they are closest to each other. Wormhole attack is the type of denial of service attack that interrupt routing operations even without the knowledge of encryptions methods The wormhole attack may be launched by a single or a pair of collaborating nodes.

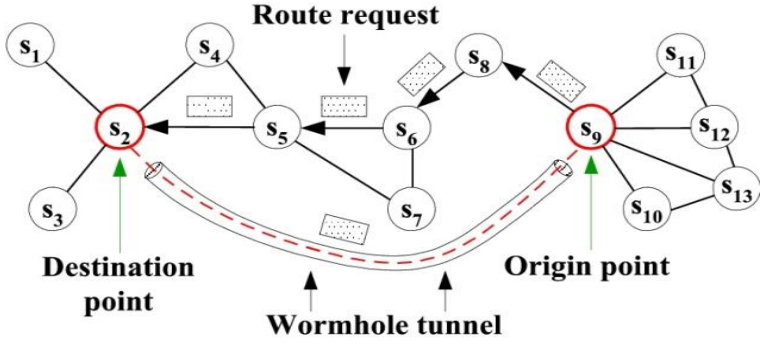

Figure 3. A wormhole attack against an on-demand routing protocol [8]

In Figure 3, we consider an on-demand routing protocol. Node s_9 wants to send data to node s_2. The adversary forwards the route request broadcasted from node s_9 via the wormhole link to node s_2 which replies with a route reply via the wormhole link. Nodes s_2 and s_9 establish a route via the wormhole link, as if they were one hop neighbours.

IV. BLACK HOLE ATTACK

Black hole is DoS attack effective on the network layer. The distinguishing property of this attack is to absorb all the data which flows through the node. If in a WSN a node is made black hole by the hacker that node will absorb all the data that comes in its range. It means if we consider a path for transmission in a WSN and the black hole node is close to the source than it will absorb all the data from the source rather than sending it to the path defined to the destination.

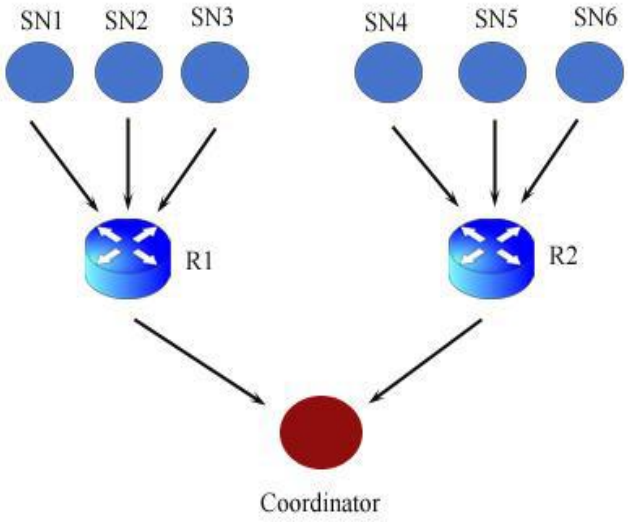

Fig 4: Normal Behaviour of Network[9]

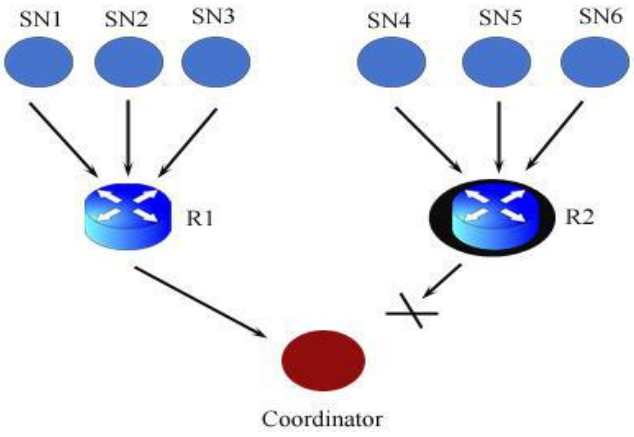

Fig 5: Black hole attack illustration[9]

Fig 4 gives the normal behaviour of the nodes where nodes R1 and R2 act as the router nodes and SN1 to SN6 are sensor nodes. Nodes SN1 to SN3 send data to R1 and remaining nodes send data to R2. The nodes are here divided into clusters. In fig 5 node R2 is made black hole and it will not forward the data received from the sensor nodes SN4 to SN6 to coordinator. In other words we can say that it will absorb all the data.

V. SYN FLOODING ATTACK

SYN flooding attacks are a common type of distributed denial-of-service attacks. The attack involves having a client repeatedly send SYN (synchronization) packets to every port on a server, using fake IP addresses. When an attack begins, the server sees the equivalent of multiple attempts to establish communications. The server responds to each attempt with a SYN/ACK (synchronization acknowledged) packet from each open port, and with a RST (reset) packet from each closed port.[10]

In a normal three-way handshake, the client would return an ACK (acknowledged) packet to confirm that the server's SYN/ACK packet was received, and communications would then commence. However, in a SYN flood, the ACK packet is never sent back by the hostile client. Instead, the client program sends repeated SYN requests to all the server's ports. A hostile client always knows a port is open when the server responds with a SYN/ACK packet[10]

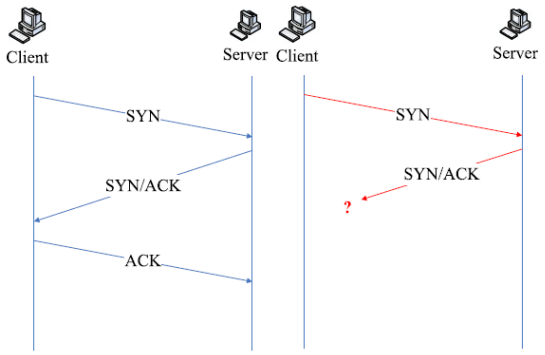

Fig 6: Normal TCP connection (left) and half-open TCP connection (right).[11]

Fig 6 depicts a normal handshake and a handshake under SYN flooding attack. As shown in the left part of Figure 6, in a normal TCP connection, a client first sends a server a SYN requesting to establish a connection. Then the server sends the client a SYN/ACK packet acknowledging receipt of the SYN packet. When the client receives the SYN/ACK packet, the client sends the server an ACK packet acknowledging receipt of the SYN/ACK packet and begins to transfer data [12].

As shown in the right part of Figure 6, in SYN Flooding attacks, attackers send SYN packets whose source address fields are spoofed. The server receiving these SYN packets sends SYN/ACK packets to spoofed addresses. If the node having the spoofed address actually exists, it sends an RST packet for the SYN/ACK packet because it did not send the SYN packet. If there is no host having the spoofed address, however, the SYN/ACK packet is discarded by the network and the server waits in vain for an ACK packet acknowledging it. For losses of SYN/ACK packets, the server has a timer in the backlog queue, and half-open states exceeding the timer are removed. When the backlog queue is filled with spoofed SYN packets, however, the server cannot accept SYN packets from users trying to connect to the server. Once all resources set aside for half-open connections are reserved, new connections cannot be made, resulting in denial of service. Furthermore, some other system resources such as CPU and network bandwidth are occupied and overloaded [13].

VI. PERFORMANCE MEASURING METRICES

- **Packet delivery ratio** :

The number of packets delivered to the destination. This illustrates the level of delivered data to the destination.

$$\sum \text{Number of packet receive} / \sum \text{Number of packet send}$$

The greater value of packet delivery ratio means the better performance of the protocol.

- **Packet Drop/ Packet Loss:**

The total number of packets dropped during the simulation.

$$\text{Packet lost} = \text{Number of packet send} - \text{Number of packet received.}$$

The lower value of the packet loss means the better performance of the protocol.

- **Average Energy:**

Power is provided to each sensor node in form of the battery either rechargeable or non-rechargeable. Sensor uses energy to sense the data, processing the data and last but not the least is transmitting the data.

Less the energy consumed by the sensor node more is the life of the node and more the data collection. It is also cost effective. Attacks drain the energy of the nodes

VII. RELATED WORK

In this work, the various modules have been implemented using Network Simulator Version 2 (ns2) in the network layer, where the mobile nodes have been established in the WSN topology. The analysis of the trace files generated by the backoff give us the PDR values during normal data flow and during Black hole, wormhole and SYN flooding attacks. PDR is different in case of all the three attacks which is discussed below.

Simulation can be performed in terms Packet delivery ratio, average energy and Packet drop.

Simulation Parameters:

Parameter	Value
Simulator	NS-2 (2.35)
Time	Blackhole=30s, Wormhole=10s and SYN flooding=12s
Total no. of nodes	15
Routing Protocol	AODV
Traffic Model	CBR
Terrain Area	800*800
Transmission Range	250m

Simulation Screenshots
Black hole Attack

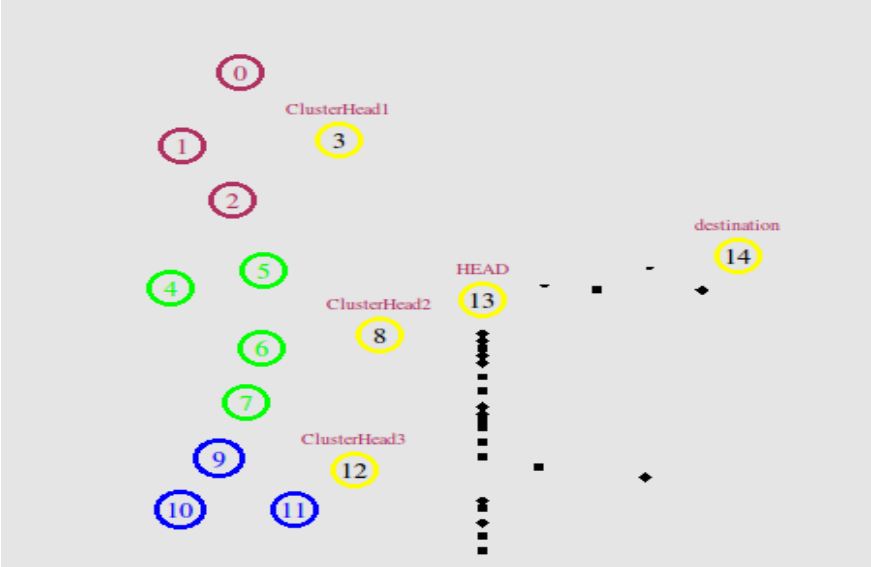

Fig 7: Black hole attack scenario

In fig 7 node 13 act as Black hole and drop the packets.

Time	Value
0	0
12	1
14	1
16	1
18	1
20	1
22	1
24	0.6219
26	0.5
28	0.83

Table 2: PDR values for blackhole attack

Table 2 contains PDR value throughout the simulation time for black hole attack. Above explains the basic property of Black hole attack. PDR values drops when attack starts i.e. 23.4 sec to 26.4 sec and later returns to normal behaviour. This only happens in black hole attack.

Wormhole Attack

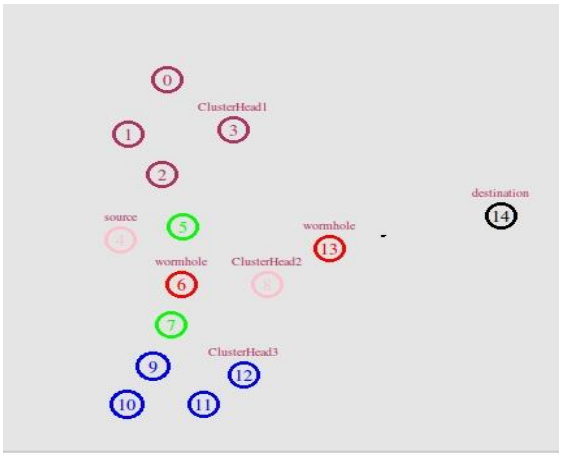

Fig 8: Wormhole Attack Scenario

In Fig 8 we consider a path from source to destination through nodes 4, 6, 8, 13 and 14. To create a wormhole tunnel we convert nodes 6 and 13 to wormhole nodes. Due to creation of a tunnel node 8 is bypassed by nodes 6 and 13. It will cause a decrease in the PDR of the network because data collected by node 8 will not be transmitted to destination.

Time	Value
0	0
2	1
6	1
6.2	0
10	0

Table 3: PDR value for Wormhole attack

Table 3 explains the behaviour of Worm hole attack. The PDR value for node 8 remains normal for 6 sec and reduces to zero during the time of attack i.e. 6.2 to 10 sec. This conclude that the node 8 is bypassed from the transmission path which is the sole characteristic of Wormhole attack.

SYN Flooding Attack

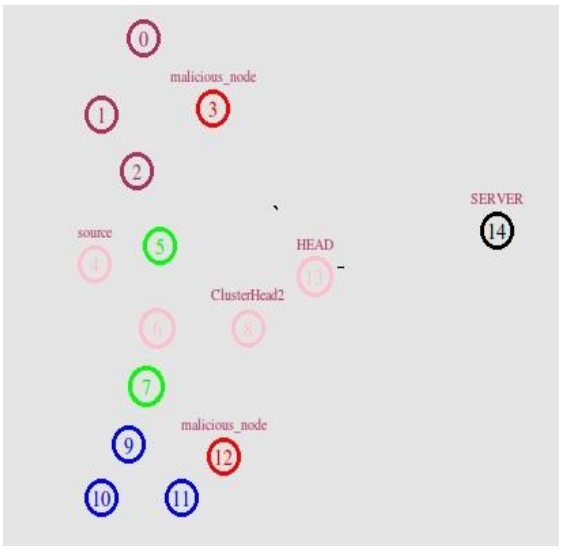

Fig 9: SYN Flooding attack Scenario

In fig 9 nodes 3 and 122 act as malicious nodes which flood the server 14 with a lot of request which prevent the legitimate user i.e node 4 to establish a connection with the server.

Time	Value
0	0
4	1
7.99	1
8	0.0192
12	0.0192

Table 4: PDR values of SYN Flooding Attack

Table 4 list the PDR values for SYN flooding attack. In SYN flooding attack PDR is calculated with respect to ACK packets send by the source before the start of the communication. During normal communication we observe that if the source send say "x" packets to the server then the server will send "x" ACK packets to the source. So PDR is 1. During the attack the PDR never goes 0.

Comparative Graph

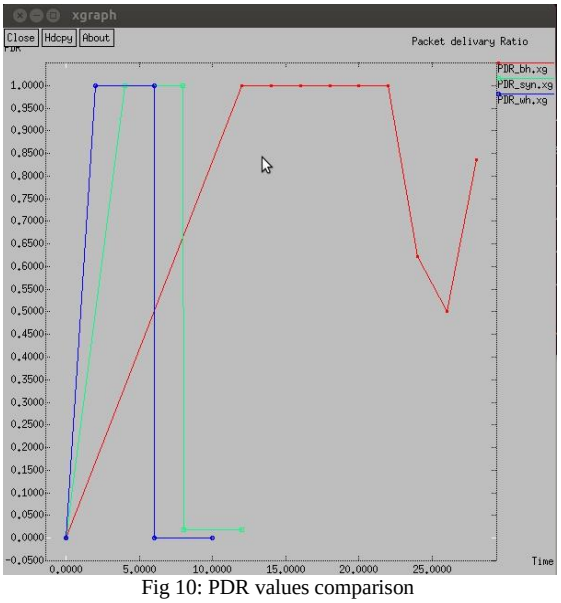

Fig 10: PDR values comparison

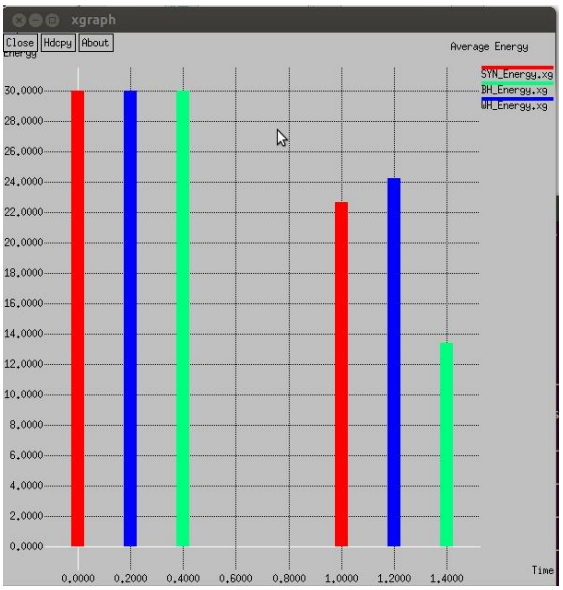

Fig 11: Comparative Energy graph

VIII. CONCLUSION

In this paper, work is done about the Wireless sensor network under blackhole attack, wormhole and SYN flooding attacks. All of these attacks have adverse effects on the QoS parameters i.e Packet Delivery Ratio, Average Energy and Packet Drop. PDR is minimum in case of Wormhole attack i.e zero. In case of SYN flooding attack the PDR is 0.0192 slightly more than Wormhole attack. Blackhole attack have a PDR nearly 0.5. Energy drop faster during the Black hole attack. In future, work can be done considering other attack analysed over other parameters like end to end delay etc. the development of secure routing protocols and new methods to detect and mitigate the effect of the above mentioned DoS/DDoS attacks.

IX. ACKNOWLEDGEMENT

I am grateful to Mr Abhinav Bhandari, assistant professor, department of computer engineering, UCoE Punjabi University, Patiala.

X. REFERENCES

[1]U. Cetintemel, A. Flinders, and Y. Sun. Power-efficient data dissemination in wireless sensor networks. In MobiDE, September 2003.

[2] N. Fultz, and J. Grossklags, Blue versus Red: Towards a Model of Distributed Security Attacks, In Financial Cryptography and Data Security, Roger Dingledine and Philippe Golle (Eds.). Lecture Notes in Computer Science, vol. 5628, Springer-Verlag, pp. 167-183, 2009, Berlin, Heidelberg.

[3] L. Greenemeier, Estonian Attacks Raise Concern Over Cyber "Nuclear Winter", Information Week, May 24, 2007,[online]http://www.informationweek.com/news showArticle.jhtml?articleID=199701774

[4] Agent based platform for the design and simulation of wireless sensor networks by Abdelhakim Hamzi, College of Computer and Information Sciences,Al-Jouf University Sakaka, KSA. Mouloud Koudil Laboratoire de Méthodes de Conception de Systèmes Ecole Nationale Supérieure d'Informatique (ESI) Algiers, Algeria.

[5] Devesh Jinwala, "Ubiquitous Computing: Wireless Sensor Network Deployment, Models, Security, Threats and Challenges", National conference NCIIRP-SRMIST, pp.1-8, April 2006.

[6] Detecting and Preventing Wormhole Attacks In Wireless Sensor Networks P. Hemalatha *ME –CSE first year IFET College of Engineering and Technology Villupuram*

[7] Mauro Conti,Roberto Di Pietro,Luigi Vincenzo Mancini, and Ales- sandro Mei,"Distributed Detection of Clone Attacks in Wireless Sensor Networks" IEEE Transaction on dependable & secure computing vol.8 n0.5 September 2011.

[8] http://www2.engr.arizona.edu/~llazos/research.php

[9] G. Vigna, S. Gwalani and K. Srinivasan, "An Intrusion Detection Tool for AODV-Based Ad hoc Wireless Networks", Proc. of the 20th Annual Computer Security Applications Conference (ACSAC'04).

[10] http://searchsecurity.techtarget.com/definition/SYN-flooding

[11] Detecting SYN flooding attacks based on traffic prediction Shangguang Wang*, Qibo Sun, Hua Zou and Fangchun Yang State Key Laboratory of Networking and Switching Technology, BeijingUniversity of Posts and Telecommunications, Beijing 100876, China

[12] Bellaiche M, Gregoire J-C. Source detection of SYN flooding attacks. Proceedings of the 2009 International Conference on Network and Service Security (N2S 2009), 2009; 1–6.

[13] Nashat D, Xiaohong J, Horiguchi S. Detecting SYN flooding agents under any type of IP spoofing. Proceedings of IEEE International Conference on e-Business Engineering (ICEBE 200), 2008; 499–505.

