DOI: 10.2298/CSIS120914029K

Traffic Deflection Method for DOS Attack Defense using a Location-Based Routing Protocol in the Sensor Network

Ho-Seok Kang[1], Sung-Ryul Kim[1,*], and Pankoo Kim[2]

[1] Division of Internet and Multimedia Engineering,
Konkuk University, Seoul, Republic of Korea
hsriver@gmail.com, kimsr@konkuk.ac.kr
[2] Department of Computer Engineering,
Chosun University, Gwangju, Republic of Korea
pkkim@chosun.ac.kr
*Corresponding Author

Abstract. As the ubiquitous computing environment gets more attention and development, WSN (Wireless Sensor Network) is getting popular as well. Especially, the development of wireless communication and sensor equipment greatly contributes to the popularization of WSN. On the other hand, the safety and security of WSN attracts lots of attention due to such a development and distribution. The DoS (Denial of Service) attack, which gets more sophisticated and broadens its domain into various services fields, may have negative effects on WSN, making it vulnerable to attacks. Since WSN collects information through sensors that are already deployed, it is difficult to have its energy recharged. When WSN is under a DoS attack, sensor nodes consume lots of energy, bringing about a fatal result to the sensor network. In this paper, we propose a method to efficiently defend against DoS attacks by modifying routing protocols in the WSN. This method uses a location based routing protocol that is simple and easy to implement. In the WSN environment where the location-based routing protocol is implemented, this method disperses the DoS attack concentration of traffic by using the traffic deflection technique and blocks it out before arriving at the target destinations. To find out the number of traffic redirection nodes proper for this method, we have performed a few experiments, through which the number of such nodes was optimized.

Keywords: sensor network, traffic redirection, filtering, location-based routing protocol, Denial of Service

1. Introduction

DoS (Denial of Service) attack is a set of methods that tries to make a target service unusable without actually hacking into the system. DoS attack has gradually developed into a method of using various attack paths as DDoS (distributed denial-of-service) attack and of attacking the entire network to which target belongs. DoS attacks can be classified into flooding, connection, and application attack types. Flooding attack can be divided into SYN/ACK flooding, TCP/IP null, FIN flooding, TCP connection, and HTTP attacks. Application attack is an attack using the characteristics of an application, and the target applications include FTP, VoIP and DNS [1]. Moreover, DoS attacks are increasing three times faster than the other attacks and are more dangerous because their implementation is relatively easier. The methods to protect against DoS attacks can be categorized roughly into four kinds: attack prevention, attack detection, attack source identification, and attack reaction [2]. Among these, the attack-prevention techniques are ways of blocking out DDoS attacks in advance, preventing them and coping with them sufficiently by locating their sources [3, 4].

DoS attacks have been limited to the existing particular networks or servers so far. However, it is recently broadening its domain to small-sized networks, such as AS and VPN, mobile networks, and even sensor networks. In fact, there has appeared a new method of DoS attack using smart phones, which actually threatens the establishment of stable mobile services. Thus, out of all the attack prevention methods, this work intends to design a system apt to defend DoS attacks in the environment of WSN, which is a network that can collect a variety of information in the ubiquitous computing environment.

WSN functions to collect a variety of information measured on particular areas, such as vehicle traffic flow, weather information, and detection systems of military or companies [5, 6]. When such a sensor network is once installed, it works independently and delivers measured information to a few sink nodes by comprising a network through connections with neighboring sensors. Each sensor node consists of a sensing device to obtain information, a processing device to process information collected, a trans-receiver in charge of communication between sensor nodes, and an electric power device to supply power. The problem is that power cannot be supplied to these sensor nodes once they are installed [6]. Therefore, they should work with as little electric power as possible in performing the collection and transmission of data as. In such a sensor network, it becomes a great weakness if each node tries to block out DoS attacks with its own filtering system, because a filtering system requires arithmetic computation which consumes a lot of energy.

In this paper, we applied the concepts of Shield [7] and sShield [8], which are traffic deflection techniques for defending against DoS attacks, to the sensor network environment with limited power. This method is a system which can distribute and block out traffic by using stepwise DoS attack detection. The detection method can be any efficient one and is not in the range of this paper. By applying deflecting techniques to the location-based routing protocol of sensor network, we attempted to make it possible to flexibly cope with DoS attacks. In this method, it is an important factor how many deflection nodes the administrator chooses. The power consumption of the deflection nodes will be higher than other normal nodes and thus it is important to select the minimum possible number of nodes that may achieve an effective defense. Therefore, in this paper, we conducted an experiment to find out the most appropriate number of nodes.

As for the composition of this paper, chapter 2 explains traffic deflection methods and sensor network protocols as a related work and chapter 3 explains the sensor network protocol suggested by this paper. Chapter 4 examines the number and location of designed systems through experiments, and chapter 5 concludes.

2. Related Works

To apply traffic deflection techniques to WSN, we apply the concepts of Shield [7] and sShield [8] that work for the wired networks. Both methods aim to defend against DoS attacks and in the systems the key point are to determine where to install the filtering nodes since the techniques work with any filtering techniques. Besides, since they change normal traffic paths by force through the modification of protocols, they are helpful in dispersing traffic also.

Both methods operate through the transformation of routing protocols. Therefore, it is needed to examine the routing protocols of WSN. Out of them, the location-based routing protocol was selected for this system because of its ease of implementation, deployment, and addition and deletion nodes.

2.1. Traffic Redirection Methods

Unlike existing DoS defense systems, Shield [7] focuses on not how to identify and block malicious traffic but on where to deploy the defense system. Briefly speaking, it makes legitimate traffic arrive at the destination even under an attack, by controlling, monitoring and even blocking out some of the traffic. Thus, Shield is implemented by using traffic trapping and traffic black-holing that are already widely used. As shown in Fig. 1, traffic trapping and traffic black-holing have a concept of having legitimate users' traffic passed through the shield but attackers' traffic blocked out by the shield, while redirecting traffic with shield nodes.

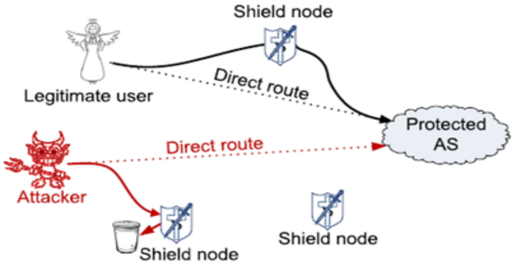


Fig. 1. Diverting traffic flow from a direct route to pass through filtering node (Shield)

There are a few shortcomings of Shield. First, Shield cannot be used inside an AS, because of its use of BGP (Border Gateway Protocol). Therefore, the Shield cannot be deployed inside an AS where small-sized DDoS attacks may occur. Second, under a DDoS attack, the traffic sent by an attacker should be blocked out, but legitimate traffic should arrive at destinations. For this, Shield cannot but provide tunneling or use some kind of source routing. When normal traffic is sent to destinations with such a method, however, there will be an increase in the overhead of a large number of nodes and the network itself.

To supplement these shortcomings, sShield [8] is designed to operate inside an AS by using the concept and definition of Shield. RIP is used as a routing protocol inside an AS. sShield assumes, as it is with Shield, the existence of effective filtering and attack filtering systems and deals with the deployment problem. Since sShield is deployed between two routers and blocks out traffic passing between the two routers, they needed to deploy several sShields and tried to optimize the number and location of sShields. Lastly, to efficiently manage the system, this work systematized sShied to operate in three phases by the riskiness of attacks.

For an efficient management of this system, sShield has three different attack modes, normal routing mode, preventive routing mode and protected routing mode. Each mode is decided by the administrator of AS, depending on attackers' attack phases. Normal routing mode is used for normal operating state where no attack is present and sShield does not do anything and thus no traffic passes through sShield. However, when traffic suspicious of attack is identified, the administrator changes the routing path to sShield, converting normal routing mode to preventive routing mode. In case of an actual attack, the administrator converts preventive routing mode to protected routing mode, in which state traffic caused by attackers is blocked out.

Normal routing mode → Preventive routing mode

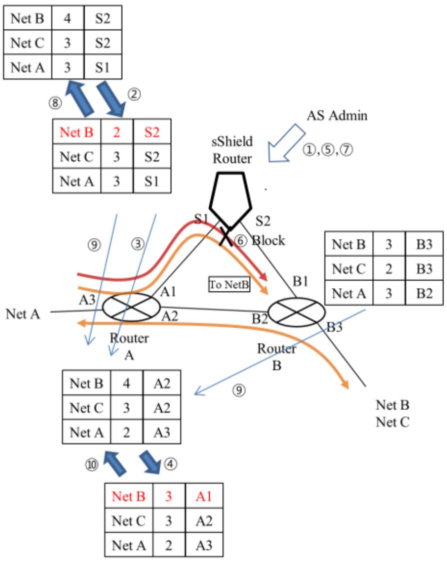
① sShield is notified by the AS that Network B is being suspected to be the target of a DoS attack
② sShield saves the content in the field to the database and set the hop count of the field to n-2
③ The routing table of sShield is sent to Router A by using triggered update
④ Routing table of Router A is changed and then traffics destined to network B is sent to sShield

Preventive routing mode → Protected routing mode

⑤ sShield is notified by the AS that Network B is being determined to be the target of a DoS attack
⑥ sShield blocks to toward to network B traffics using filtering rules

Return to Normal routing mode

⑦ When DoS Attack stop, AS change mode to Preventive routing mode/Normal routing mode
⑧ sShield restores routing table in the database
⑨ sShield and Router B send routing update messages to router A
⑩ The routing table of Router A is changed to original table



Net B	4	S2
Net C	3	S2
Net A	3	S1

Net B	2	S2
Net C	3	S2
Net A	3	S1

Net B	3	B3
Net C	2	B3
Net A	3	B2

Net B	4	A2
Net C	3	A2
Net A	2	A3

Net B	3	A1
Net C	3	A2
Net A	2	A3

Fig. 2. Changing routing tables of sShield's three routing modes

Fig. 2 shows the process of mode chamges in sShield system. This sShield system also suggested a method to determine the location of attack defense systems deployed, and this structure can be deployed in any position. sShield can be deployed and work inside an AS by using RIP (Routing Information Protocol), which is a typical protocol of IGP (Interior Gateway Protocol) [9]. In other words, it is able to prevent small-scaled DDoS attacks likely to occur inside an AS. Besides, in cooperation with Shield, it is possible to deploy the technique in any position on the internet, and since it uses RIP, traffic unblocked out can reach its destination. More importantly, sShield using the table update of RIP can deflect and block out paths by the unit of networks being attacked, so it is possible to control the flow in a precise way. Lastly, the other existing routers do not have to know the existence of sShield, and routers do not have to be replaced at all, which helps keeping the consistency of a network.

In this paper, we developed a new DoS defense system by applying these traffic deflection ideas to wireless sensor networks.

2.2. Sensor Network Routing Protocols

Routing in WSN is different from ordinary routing protocols used in the existing wired network. Important factors include: nonexistence of infrastructure, unreliability of wireless links, and high probability of errors for many sensor nodes. What matters most is all the routing protocols should save energy to work without being recharged again [5, 6]. To satisfy these conditions, there have been many different routing protocols made for WSN, and these protocols can be largely classified into six categories as shown in Table 1.

Table 1. Routing protocols for WSN

Category	Representative Protocols
Location-based Protocols	MECN, SMECN, GAF, GEAR, Span, TBF, BVGF, GeRaF
Data-centric Protocols	SPIN, Directed Diffusion, Rumor Routing, COUGAR, ACQURE, EAD, Information-Directed Routing, Gradient-based Routing, Energy-aware Routing, Information-Directed Routing, Quorum-Based Information Dissemination, Home Agent Based Information Dissemination
Mobility-based Protocols	SEAD, TTDD, Joint Mobility and Routing, Data MULES, Dynamic Proxy Tree-Based Data Dissemination
Hierarchical Protocols	LEACH, PEGASIS, HEED, TEEN, APTEEN
Multipath-based Protocols	Sensor-Disjoint Multipath, Braided Multipath, N-to-1 Multipath Discovery
Heterogeneity-based Protocols	IDSQ, CADR, CHR
QoS-based protocols	SAR, SPEED, Energy-aware routing

Such multitude of sensor network protocols has been developed to fit the way and purpose of each different kind of WSN. Data-centric protocols are designed for the purpose of sending data to sink nodes [10, 11, 12]. Hierarchical protocols work by building up sensor nodes in a hierarchical way [5, 6]. Mobility-based protocols are for circumstances when sink nodes move [6]. Multipath-based protocols are to build up several paths from source to sink nodes, not just one single path [6]. Heterogeneity-based protocols are designed for the sensor network environments that combine battery-based sensor networks and power-supplied sensor networks [5, 6]. QoS-based protocols try to minimize the consumption of energy [5, 6]. Lastly, location-based protocols deliver information using the physical locations of nodes as part of routing information, where the physical location of each node is assumed to be known by the nodes [5, 6, 13].

The next explanation is about greedy-based protocol [13], which is the simplest one out of all the location-based protocols. When any sensor network is first deployed, it informs all the nodes of its physical location. All nodes have the physical location table with location information of entire nodes. Besides that, each node should be aware of other nodes within its communication range as well. In this way, when a node attempts to send data to a particular node, it sends data to another node in its communication range, which is located nearest its destination. Fig. 3 shows the process of sending data from node x to node d. Node x sends data to its destination x, through node a. At this point, Node a, having received the data, selects node b, among b, s, x located within its communication range, to transfer data, which is physically proximate to node the destination node d.

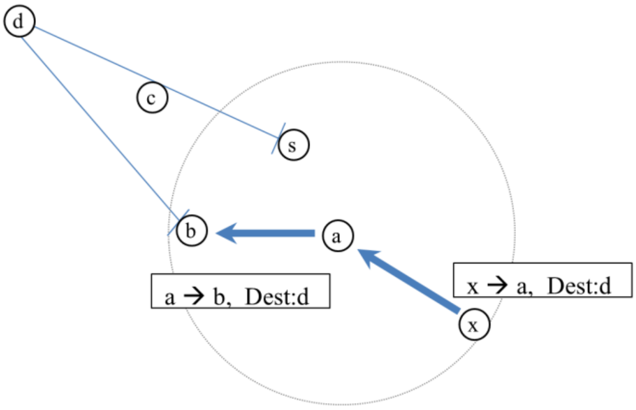


Fig. 3. Location-based routing protocol

2.3. Protection of DoS Attack in WSN

The existing DoS defense methods in WSN were mostly to block the zombie node generation in nodes with authentication by sensor nodes [14, 15, 16], to classify and block services in [17] network traffic, or to select DoS attacks by measuring incoming traffic volume via a sink node [18]. All these methods try to prevent DoS attacks at the source (by authentication or service block) or at the sink and there is no discussion about how to deflect traffic when DoS attacks cannot be prevented that way.

The Shield [7] and sShield [8] are methods to handle exactly that problem in fixed network. However, [7] and [8] work as fixed network routing protocols such as RIP and BGP. In order to apply the idea to WSN, we devised a method for location-based routing protocol, which has the simplest concept among WSN protocols.

3. New DoS Defense System in WSN

In building the suggested protocol, we have made the assumptions listed in the following subsection. Also, we will explain how to distinguish the location where the attacker is located. After explaining all of them, we will explain DoS defense methods in WSN by three phase modes similar to sShield. The three phase modes are normal mode, preventive mode and protected mode.

3.1. Assumptions

- The network of interest is a sensor network structure where free data communication is provided without the concepts of sink and source. However, the system works even in an ordinary sensor network with sink and source nodes.
- The routing protocol for this system is greedy-based routing protocol which is the most basic out of all the location-based protocols.
- Being equipped with GPS, all the nodes know their own locations and each node are also provided with a unique node number. When first deployed, the node numbers are broadcast to the entire nodes.
- The nodes renew information about their neighboring nodes and physical locations on a regular basis. It is to notice any change in neighboring nodes' circumstances. It is possible to have node failures, power exhaustions, and node additions.
- There exists an administrator controlling detection of DoS attacks, selecting nodes, making traffic deflection, and changing modes.
- The nodes in charge of traffic deflection are called ssShield (selected sensors for Shield) nodes in this paper.
- Depending on the riskiness of DoS attack against the sensor network, there exist three modes of operation similar to those of sShield, which are normal, preventive, and protected modes.

3.2. Attacker

The following are the nodes or methods that are likely to lead to a DoS attack in WSN.

- Attacks made through the sink node from an external node.
- Internal sensor nodes deployed inside WSN.
  A new sensor node deployed by an attacker for DoS attack.

3.3. Three Phase Modes

The administrator manages DoS attack situations by dividing them into normal mode, preventive mode, and protected mode. Normal mode indicates a stable state without any attacks. When finding out information suspicious of DoS attack coming through several different paths, the administrator changes normal mode to preventive mode, which redirects traffic to the destination in preparation for a DoS attack. When the deflection traffic turns out to be a DoS attack, the administrator changes the mode to protected mode, which blocks out traffic to the destination.

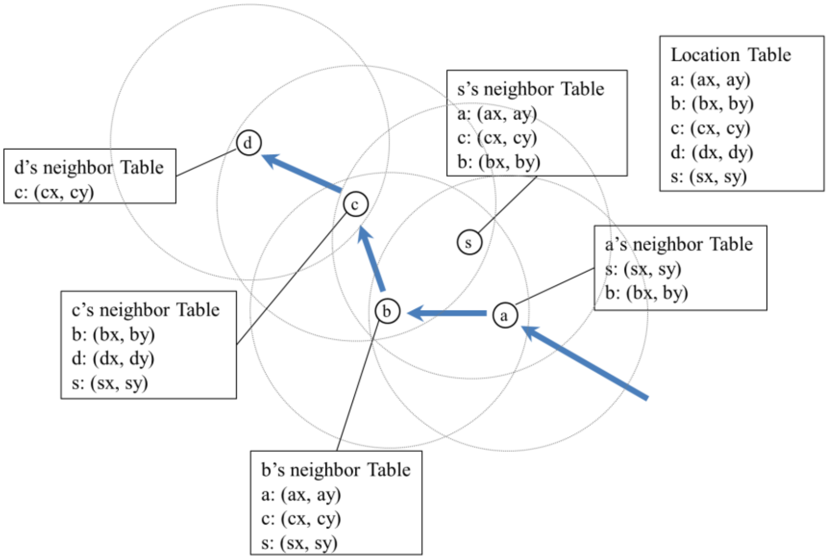


Fig. 4. Sensor network architecture (Normal mode)

Fig. 4 shows a part of the sensor network using the location-based routing protocol. This figure explains how these three modes work. The symbols a, b, c, d, and s indicate each sensor node's number and the grey circle indicates the communication range of each node. Location table is a table with every sensor node's physical coordinates. Moreover, each sensor node has information about its neighboring node to communicate. Fig. 4 shows a state of normal mode and how traffic headed for node d is delivered through other nodes.

At this point, when collecting information suspicious of a DoS attack on node d, the administrator selects some nodes out of all the sensor nodes as ssShield nodes and commands them to change their mode to preventive mode. That is, any node can be an ssShield node, but when they are not selected as ssShield nodes by the administrator, they do not know which nodes are ssShield ones. Fig. 5 shows how node s is selected as ssShield node. The first thing ssShield node does is monitoring all the traffic existing in its communication range. Then, it looks to see if there is traffic heading for node d which is suspected of a DoS attack. If there is traffic heading for node d, it informs that its location has changed in order to bring the traffic to node s. Fig. 6 shows the process of traffic going through node s due to the modified location of s. This Preventive mode works only as distributing suspicious traffic and can be useful for collecting suspicious traffic for further analysis.

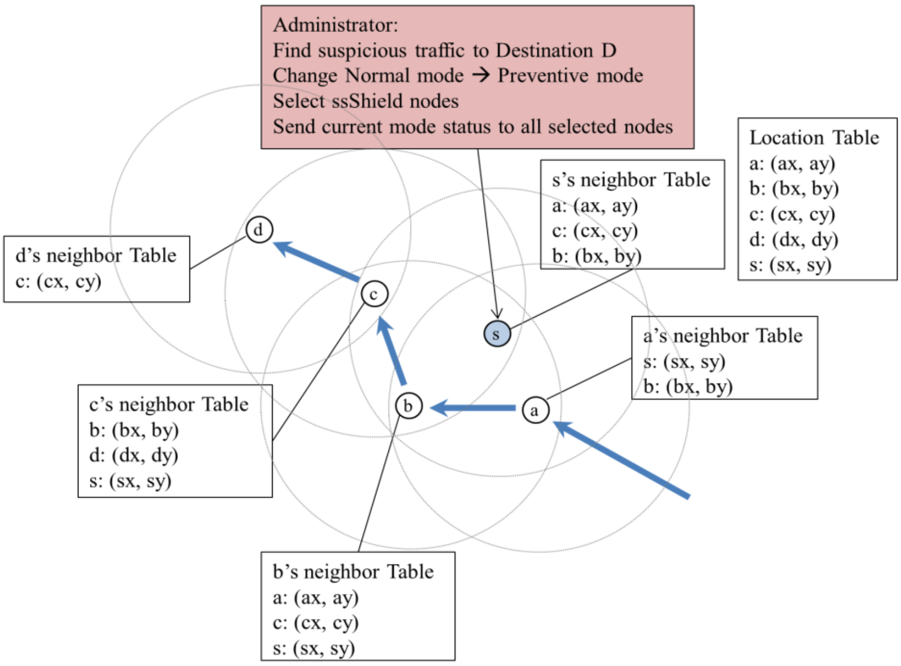


Fig. 5. Change Normal mode to Preventive mode

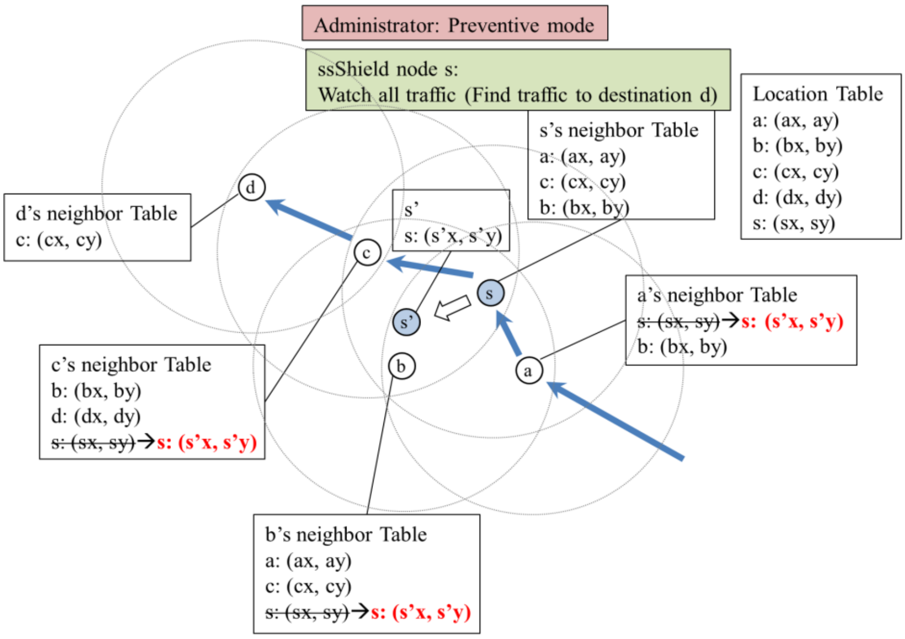


Fig. 6. Traffic redirection by location change

When this traffic is found to be a DoS attack, the administrator commands all the ssShield nodes to block out traffic heading for node d, as shown in Fig. 7. When the DoS attack stops, the administrator makes the ssShield nodes return not to normal mode right away, but to preventive mode first. Then, if there does not occur a DoS attack for a certain period of time, all the ssShield nodes return to normal mode while informing neighboring nodes of their physical locations, as shown in Fig. 8.

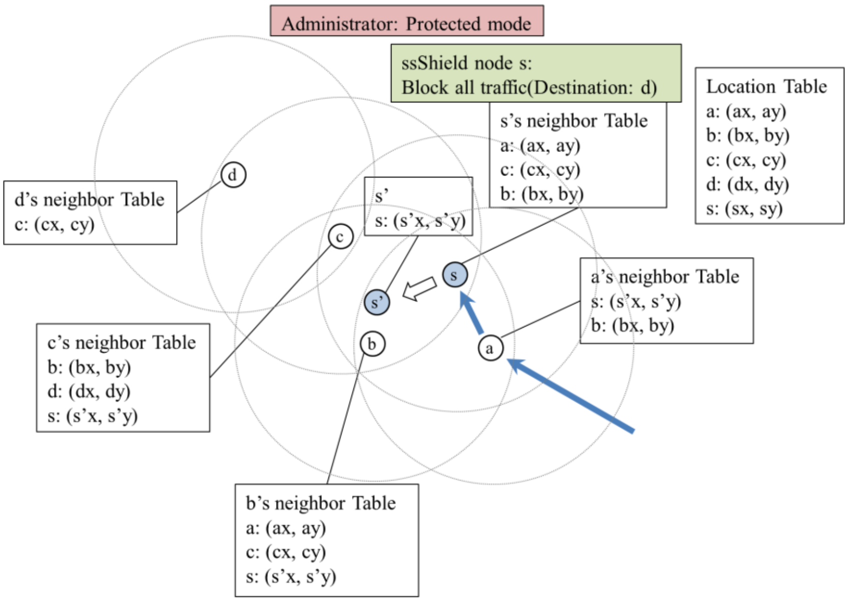


Fig. 7. Protected Mode

3.4. Pros and Cons of this System

ssShield is a system apt to disperse and block out traffic caused by a DoS attack in WSN where the location-based routing protocol is used. While being controlled by the administrator, ssShield can execute the dispersion and block-out of traffic at the same time by deflecting traffic caused by a DoS attack. Some pros and cons of ssShield will be discussed in the following.

As for its advantages, it is possible to efficiently manage energy. First, since a filtering system need not be put on the sensor node, it is possible to prevent waste of energy caused by arithmetic operation. Besides, it is possible to disperse electric power consumption concentrated on particular nodes, caused by a DoS attack. Second, other nodes that are not selected as ssShield nodes do not have to perform such operations as deflection and block-out of traffic. They do not have to be controlled by the administrator, while keeping the consistency without the need of the existing protocols to be modified.

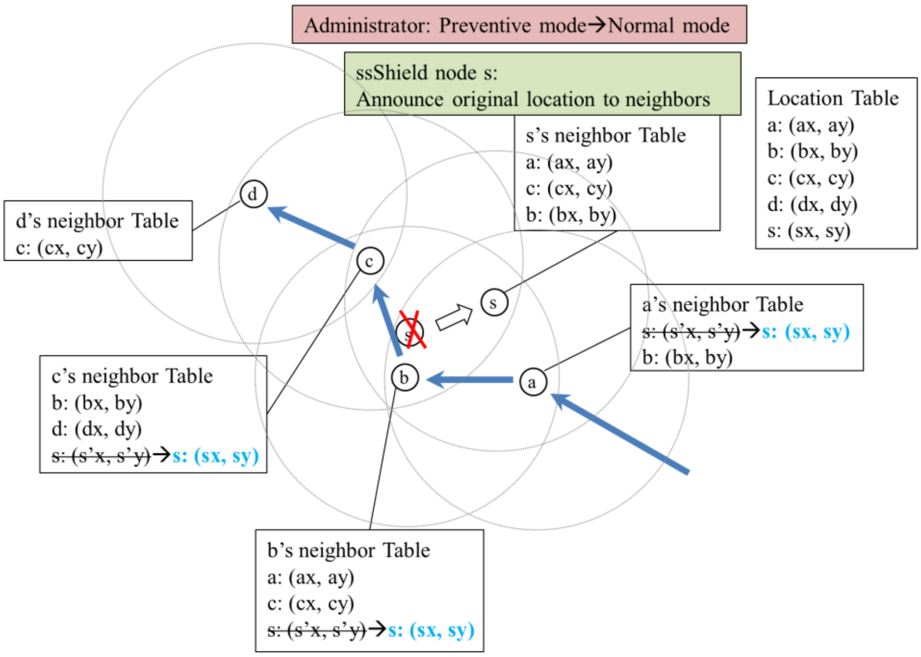


Fig. 8. Return to Normal mode

As for its disadvantages, first, it must redirect and block out both the legitimate and malicious traffic heading for the target nodes of DoS attack. The reason is that there is no way to distinguish the malicious traffic from legitimate traffic unless filtering modules are put on sensor nodes selected as ssShield nodes. Second, sensor nodes selected as ssShield nodes have a higher power consumption rate than other nodes. The energy consumption increases during the process of inspecting all the signals around nodes to make traffic deflection. However, it is still lower than when the WSN is under DoS attack, in terms of the mean energy consumption of sensor nodes. Third, when a traffic redirection should be made in the preventive mode, there may be some cases when traffic cannot be delivered to destinations, depending on the circumstances of sensor nodes. In case when traffic comes to ssShield itself, the ssShield node should cancel path deflection while judging whether its connection is disconnected. Lastly, since modifying physical locations is similar to a malicious activity, it is required to provide a safe key mechanism between the administrator and every sensor node.

4. Experiments

Through an experiment, we attempted to investigate the defense rate of DoS attacks by the number of ssShields. This experiment is to find out how many sensor nodes the administrator should select in order to defend a DoS attack efficiently.

4.1. Experiment Environment

The experimental environment is a simulated one and the topology of sensor nodes was determined randomly. We fixed the number of sensor nodes, the communication range of sensor nodes, and the entire width without any change given. For the experiments, ten times of topology change was made for each round, and twenty times of ssShield selection was made for each topology. At the same time, twenty times of DoS attack was performed while ssShield was arranged one time, through which this system marked the probability that ssShield could defend DoS attacks. For a DoS attack, traffic was arbitrarily caused in randomly selected nodes to attack randomly selected set of nodes. The nodes selected as "ssShield" by Administrator are determined by random selection method. If ssShield nodes are selected by a specific criterion, then there is a high probability of a biased choice which will lead to concentration of energy consumption to specific nodes, which, in turn, will shorten the time the whole network is useful. The possibility remains that some clever mechanism exists that do not have this drawback, but it is left as a future work.

4.2. Result of Simulation

At first, the experiment was performed by increasing by two ssShields nodes to the topology deployed with 100 wireless sensor nodes in WSN environment.

Fig. 9 shows the probability of successfully defending DoS attacks by the ratio of ssShields selected. This experiment used the topology deployed with 100 nodes, and an average of 3.8 nodes existed in the communication range of any single node.

As shown in Fig. 9, when 50% of all wireless sensor nodes were selected, the traffic dispersion and filtering can be provided against DoS attacks most of the time. However, it means that 50% of the entire sensor nodes consume power more than in a normal state. Therefore, it is necessary to select a right number of nodes fit for the sensor administrator's policy and network circumstances.

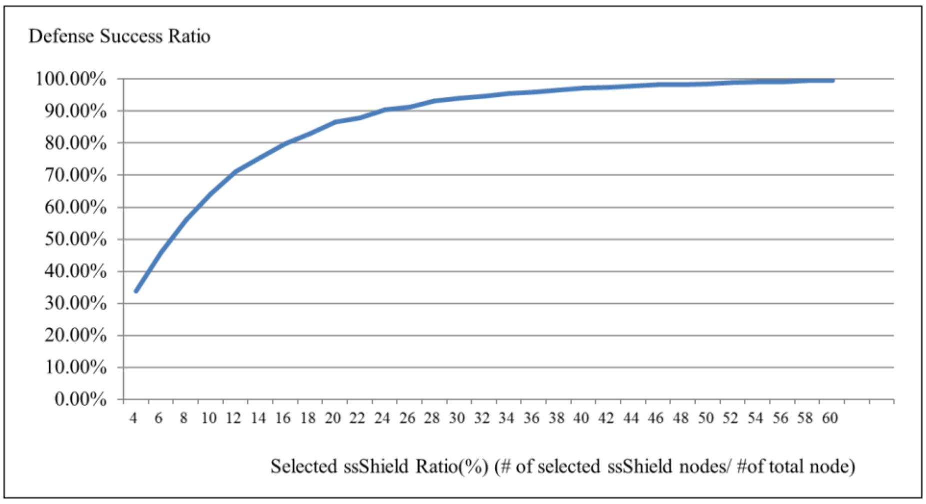


Fig. 9. Probability of defending DoS attack by the ratio of ssShields selected

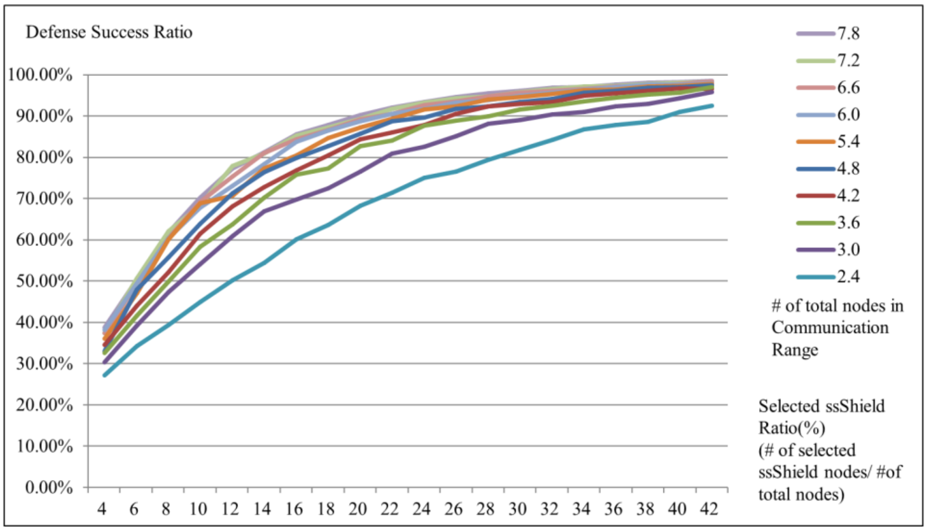


Fig. 10. Probability of defending DoS attacks by an increase of the entire sensor nodes

Fig. 10 is a graph showing how the defense ratio changes against DoS attacks as the number of wireless sensor nodes deployed in the same space increases. As shown in this graph, it is clear that the defense capability depends on the distance between sensor nodes, in other words, how many neighboring nodes there are in one communication range.

5. Conclusion and Future Works

In this paper, we proposed a new method to defend against DoS attacks in WSN using the ideas of Shield and sShield that are DoS attack defense techniques using traffic deflection for the existing wired networks. Out of the wireless sensor network routing algorithms, this paper focused on the location-based routing protocol for the sensor network environment since it is simple and easy to implement and install. The proposed method was systematized with three phases of DoS attacks fit for each risk circumstance, and the administrator was made to select nodes to make traffic deflection when judging a DoS attack. Then, by changing the location parameter of location-based routing protocol only for nodes selected, it is possible to for the selected nodes to make traffic come to themselves, by which a DoS attack could be blocked out. Besides, the number of nodes to deflect path was confirmed by experiments. By using the results, it will be possible to make judgments about the appropriate number of nodes depending on various sensor network conditions. This paper proposed a method to defense DoS attack effectively in WSN (wireless sensor network) environment by using traffic diversion method.

Traffic deflection was applied only to the location-based routing protocol in this paper. Therefore, it is necessary to examine if this method can be applied to other protocols. Moreover, no exact experiment was conducted on the consumption of energy. However, it is expected to measure energy consumed in an entire sensor network by using traffic loaded on the entire nodes in each mode. Sensor nodes were randomly selected for path deflection. This is to prevent energy consumption from concentrating on a specific node, but there may be other methods possible too. Probably, we may consider to use nodes around the sink node, an concentrated spot, or nodes consuming the least amount of energy. All these comprise possible future works.

Acknowledgments. This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST) (No. 20120006492).

References

1. Tao peng, Christopher Lecke, Kotagiri Ramanohanarao.: Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems. ACM Computing Survey(CSUR) vol.39, no.1, Article 3. (2007)
2. K Gar.: Detection of DDoS attack using data mining. International Journal of Computing and Business Research (IJCBR) volume 2 Issue 1. (2011)
3. Trustwave SpiderLabs.: The Web hacking incident database Semiannual report. July to December. (2011)
4. E. Kline, M. Beaumout-Gay, J. Mirkovic, and P. Reiher.: RAD:Reflector attack defense using message authentication codes. In Proceedings of Annual Computer Security Applications Conference(ASAC). pp. 269-278. (2009)

5. Shio Kumar Singh, M P Singh, and D K Singh.: Routing Protocols in Wireless Sensor Networks – A Survey. International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.2. (2010)
6. Kemal Akkaya, Mohamed Younis.: A survey on routing protocols for wirless sensor network. Ad Hoc Networks Vol. 3, Issue 3. (2005)
7. Erik Kline, Alexander Afanasyev, Peter Reiher.: Shield: DoS Filtering Using Traffic Deflecting. 19th IEEE International Conference on Network Protocols (2011).
8. Ho-Seok Kang, Sung-Ryul Kim.: Design and Experiments of small DDoS Defense System using Traffic Deflecting in Autonomous System. Journal of Internet Services and Information Security(JISIS) In proceedings of MIST 2012, Vol.2, no.3,4. pp.43-53 (2012)
9. James F. Kurose, Keith W. Rose, Computer Networking.: A Top-Down Approach Featuring the Internet. Addison Vesley Longman Inc. (2001)
10. C. Intanagonwiwat, R. Govindan, and D. Estrin.: Directed diffusion: A scalable and robust communication paradigm for sensor networks. Proceedings ACM MobiCom'00, Boston, MA, Aug. pp. 56-67. (2000)
11. C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva.: Directed diffusion for wireless sensor networking. IEEE/ACM Transactions on Networking. vol. 11., no. 1. (2003)
12 D. Braginsky and D. Estrin.: Rumor routing algorithm in sensor networks. Proceedings ACM WSNA. in conjunction with ACM MobiCom'02 GA, pp. 22-31. (2002)
13. Brad Karp, H.T. Kung.: GPSR: Greedy Perimeter Stateless Routing for Wireless Network. MobiCom. (2000)
14. Yao Lan, Yu Zhiliang, Zhang Tie, and Gao Fuxiang.: Dynamic window based multihop authentication for WSN. In proceedings of 17th ACM conference on CCS'10. pp. 744-746 (2010)
15. Hao Chen.: Efficient compromising resilient authentication schemes for large scale wireless sensor networks. In proceedingds of 3rd ACM conference on WiSec'10. pp.49-54 (2010)
16. Chakib Bekara, Maryline Laurent-Maknavicius and Kheira Bekara.: H^2BSAP: A hop-by-hop Broadcast Source Authentication Protocol for WSN to mitigate DoS attacks. In proceedings of 11th IEEE Singapore International Conference on ICCS 2008. pp.1197-1203 (2008)
17 Jiang Zhongqiu, Yan Shu, and Wang Liangmin.: Survivability Evaluation of Cluster-Based Wireless Sensor Network under DoS Attacks. In proceedings of 5th International conference on WiCom'09. pp.1-4. (2009)
18 Khusvinder Gill and Shuang-Hua Yang.: A Scheme for Preventing Denial of Service Attacks on Wireless Sensor Networks. In proceedings of 35th IEEE Annual Conference on IECON'09. pp.2603-2609. (2009)

Ho-Seok Kang is a postdoctoral fellowship of the division of Internet and Multimedia Engineering at Konkuk University, Seoul, Korea. He received his Ph.D. degree in computer enginnering at Hongik University, Korea. His recent research interests are in network security, network protocol, mobile security, distributed algorithms and cloud computing.

Sung-Ryul Kim is a professor of the division of Internet and Multimedia Engineering at Konkuk University, Seoul, Korea. He received his Ph.D. degree in computer enginnering at Seoul National University, Korea. His recent research interests are in cryptographic algorithms, distributed algorithms, security in general, cloud computing, and data mining.

Pankoo Kim received the B.S. degree in computer engineering at Chosun University, the M.S. and the Ph.D. degree in computer engineering at Seoul National University in South Korea. He is a professor in the Department of Computer Engineering at Chosun University. His research focuses on Semantic Web Technologies, Ontology, Multimedia, Natural Language Processing, and Data Mining.

Received: September 14, 2012; Accepted: March 12, 2013