Impact of High-Mobility Radio Jamming in Large-Scale Wireless Sensor Networks

Chulho Won, Jong-Hoon Youn, and Hesham Ali

Computer Science Department
University of Nebraska at Omaha
Omaha, NE 68182, USA
{cwon, jyoun, hali}@mail.unomaha.edu

Abstract. Denial-Of-Service (DOS) attack is recognized as a biggest threat against the operation of large-scale wireless sensor networks (WSN). Especially, high-mobility radio jamming like vehicles carrying radio jamming device can cause a serious damage in performance of WSNs. Because of resource-constraint design of sensor node, it is hard to provide enough protection against high-mobility jamming attack. Therefore, large-scale WSNs are extremely vulnerable to that type of DOS attack. Recognizing the importance of the problem, we conducted a simulation study to investigate the impact of radio jamming on the performance of a large-scale WSN. Based on the simulation results, the moving speed of radio jamming source has the most conspicuous effects on the WSN performance such as packet delivery success ratio and delay. As the speed changes from 8 m/sec to 1 m/sec, the success ratio drops by up to 10 %. On the other hand, the delay increases by up to 55 %.

1 Introduction

There is an increasing demand on the use of large-scale sensor networks. Some of challenging applications include medical care, emergency response, wildlife monitoring, environmental monitoring, traffic monitoring, battlefield military operations, remote terrain exploration, and many others.

Denial-Of-Service (DOS) attack [10], [11], [12] is recognized as a biggest threat for the operation of mission-critical network. When a large-scale sensor network operates in a hostile environment, protection against DOS attacks becomes the most important issue for the longevity of system operation. Radio jamming, by a definition, is the operation of sending strong signals on the same channel or frequency to make impossible to receive desired signals. In this paper, high-mobility radio jamming is defined as a DOS attack by radio jamming device carried by an automotive mechanism such as mobile robot or vehicle. Therefore, they can cause a significant disruption of network communication in a large area of the system deployment because the mobile radio jamming can move from one location to another in a short time. Even though it is relatively easy to launch attack using high-mobility radio jamming, it is hard to provide protections against the attack.

Large-scale WSN has a weakness in protection against high-mobility jamming attack for several reasons. First, since sensor nodes are highly resource-constrained, it

X. Zhou et al. (Eds.): EUC Workshops 2006, LNCS 4097, pp. 244 – 251, 2006.

is not affordable to provide full-fledged security measures on the small-footprint sensor nodes. Second, large-scale WSNs need to operate in an unattended manner. Providing maintenance to large-scale networks is not almost possible. Therefore, a sudden change of operating conditions critically affects the system function and life time. For example, radio jamming attack causes a large amount of transmission failures in the attack area. Therefore, the sensor nodes in the attack area suffer from excessive energy consumption. Third, high-mobility radio jamming has not been much addressed in the context of WSN. There are few protection mechanisms proposed in considering the scarce resource of sensor nodes and the high-mobility of radio jamming.

Since the radio jamming creates routing voids in the WSN, the existing approaches [5], [6] for routing void can provide a solution. However, those existing approaches are not effective for high-mobility jamming. First, the existing approaches are based on the availability of the map of routing voids. In comparison, the routing voids created by radio jamming are extremely time-varying and thus the status of routing void is changed frequently in an unpredictable way. As the map of routing voids is changed quickly, the frequency of the map update needs to be increased. And thus this approach needs a significant increase of energy consumption. Since a WSN may have a very tight energy budget, frequent map update does not become a viable solution.

The main motivation of this paper is to look into the impact of high-mobility radio jamming on WSN performance by focusing on three aspects. First, high-mobility jamming attack model is developed based on key parameters such as interference range, speed, and mobility. Second, simulation is used to investigate the effectiveness of the existing routing protocols in protecting WSN against high-mobility radio jamming. Several performance metrics are measured to compare the effectiveness among the protocols. Finally, we propose a desirable approach for protecting WSN against that type of DOS attack based on the simulation results.

The rest of paper consists of as follows; Section 2 presents related work, Section 3 describes a high-mobility radio jamming model, Section 4 presents the simulation environment and the results, and finally Section 5 discusses conclusions.

2 Related Work

Research issues on DOS attack was not studied much in the context of WSN. In the positional paper, Wood [10] presented a number of different types of DOS attack, which can be used in the context of WSN. Ahmed [12] surveyed potential DOS attacks and pointed out that radio jamming on mobile machine can be an effective attack to WSN.

Several researches addressed radio interference effect in the context of short-range wireless networks. Crossbow Technology Inc. [3] and Steibeis-Transfer Center [15] independently conducted experiments to measure the effect of interference on 802.15.4. The technical document [3] from Crossbow Technology Inc. describes measurement results showing that the packet delivery rate in a MICAz sensor network

is dropped significantly by the interference with 802.11b WLAN when they use closely located radio channels. The Steibeis-Transfer Center [15] also conducted a measurement study using commercial devices. According to the study, the radio interference effect of 802.11b can cause significant performance degradation to 802.15.4. Howitt [16] analyzed the radio interference of 802.15.4 on 802.11b. He used both analysis and measurement to prove that the 802.15.4 has little or no effect on 802.11b performance and thus the coexistence of 802.15.4 and 802.11 needs to be approached to protect 802.15.4. Howitt [17] studied the effect of interference using experiments and analytical models. The experiments intended to evaluate the impact of the interference between Bluetooth and 802.11b. He also built analytical models for the interference caused by 802.11b on Bluetooth and for the interference caused by Bluetooth on 802.11b. Golmie [18] proposed a dynamic scheduling algorithm for Bluetooth to relieve the radio interference effect between Bluetooth and WLAN. The algorithm is to guarantee system performance requirements such as QoS while reducing the effect of the interference by WLAN. It extends the Bluetooth channel hopping mechanism in a dynamic way that devices in the network maximize their throughput and get the fairness of access.

As mentioned earlier, several algorithms were proposed for bypassing permanent routing voids in mobile ad-hoc networks and wireless sensor networks [5], [6]. Although the existing mechanisms are effective for permanent routing voids, radio jamming attacks creates temporary routing voids, which frequently changes the status between disconnection and connection. Therefore, the main concern of using the existing routing void mechanisms is in their low effectiveness.

Wood [11] addressed a Denial-Of-Service (DOS) attack in the context of large-scale wireless sensor network. The attack is assumed to use radio interference, called radio jamming attack. They propose a mapping and detection algorithm for jammed regions of sensor network. The mapping protocol provides the application layer the map of the jammed regions hole, which helps to route packets around the jammed regions. The detection and mapping algorithm is executed in a distributed manner. The wireless nodes in jammed region detect a jamming attack autonomously and broadcast the attack to their neighbors to detect and map the jammed area. They proposed a carrier sense defeat mechanism for broadcasting high-priority attack message.

3 High-Mobility Radio Jamming Model

For modeling a radio jamming attack, a general transmission loss model of radio signal is adopted as described in [7]. The interference signal strength at a distance of r is represented as in Equation1, where G is a random noise.

$$E(r) = m(r) + G_{\partial}$$
$$m(r) = 10\log(\frac{r}{R})^{-\alpha}, \alpha = 4, \partial = 7dB \quad (1)$$

This model shows that the interference strength, which is called intensity hereafter, is inversely proportional to the distance from the jamming source as shown in Equation (1). A circle of interference area will be formed at a distance. In that area, the jamming signal causes interference to the communications between sensor nodes. Mobility is another cause of system performance degradation under mobile radio jamming. As the jamming source moves around, the routing void changes its location. Therefore, the mobility effect is characterized by two parameters: moving speed and recurring interval. The recurring interval indicates how often the radio jamming attack returns back to the same area again. The moving speed indicates how fast the radio jamming moves through the area. To capture the general characteristics of radio jamming effect, our radio jamming model has three main parameters: interference intensity, moving speed, and recurring interval.

4 Simulation

4.1 Methodology

To evaluate the effectiveness of the proposed scheme in a large-scale sensor network, a simulation study was conducted. We used the NS2 simulator with 802.15.4 model developed at the City University of New York [13]. The WSN consists of 200 nodes and they are placed 8 meter apart on a grid.

The radio jamming effect was modeled using three parameters: intensity, speed, and interval. We assumed that there is a single source of radio jamming and all the nodes in same interference area are interfered at the same level. The intensity of the model indicates how many nodes are interfered by the radio jamming. Therefore, the higher the intensity is, the more nodes get the interference. For the mobility pattern, the radio jamming source moves at a fixed speed through the network towards to the boundary of the network. The source returns back to the old place at an interval.

For the packet traffic generation, eight pairs of sender and receiver are used for one-to-one traffic with UDP packets. The senders and the receivers are located on the opposite side of the grid. The radio jamming source moves around the space between the senders and the receivers. Each sender sends packets to its receiver at interval of 1 second.

The effect of mobility radio jamming on WSN performance was measured with two metrics: average packet delivery success ratio and average delay. The success ratio is the number of received packets divided by the number of sent packets. The delay is the time for packet to travel from sender to receiver. The metrics were measured by varying three parameters: intensity, interval, and speed. The WSN uses two popular routing algorithms: AODV (Ad-hoc On-Demand Distance Vector) [4] and GPSR (Greedy Perimeter Stateless Routing) [5].

4.2 Results

The first set of simulation results presents the effect of interference intensity on the performance of the chosen routing protocols. For the simulations, we used fixed

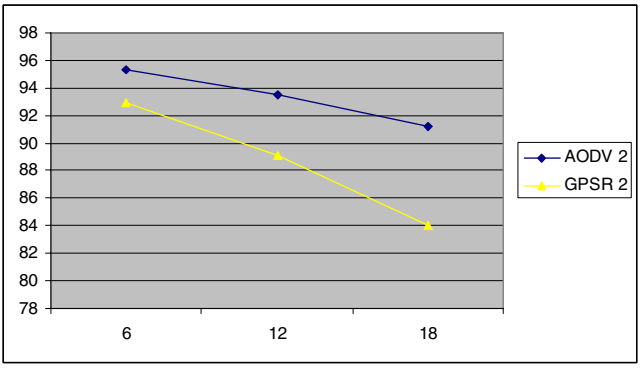

Fig. 1. Success Ratio versus Intensity

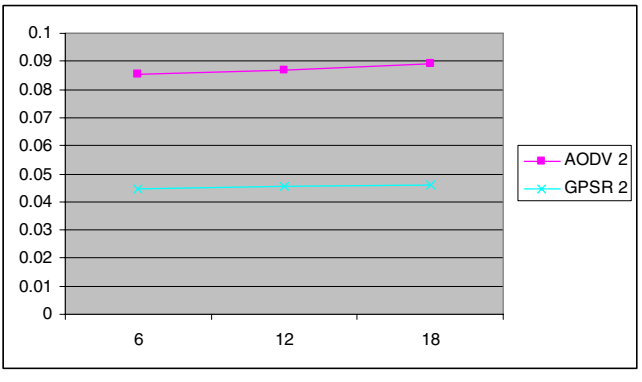

Fig. 2. Delay versus Intensity

values for the interval and the speed; the interval was set to 70 seconds and the speed was at 2 m/sec. In Fig.1 and Fig.2, AODV 2 and GPSR 2 use the speed of 2 m/sec. The intensity was set to 6 m, 12 m, and 18 m.

Fig.1 compares the success ratio between two routing protocols: AODV and GPSR. The x-axis indicates the intensity of radio jamming. The intensity represents the radius of the interference area. It is interesting to note that two protocols react to the change of the intensity differently. AODV adapts quickly to the change of the intensity. Therefore, the protocol maintains its performance pretty well. In comparison, GPSR shows a rapid degradation of performance over the change of the intensity. It is because it needs to wait for a long time until the routing information is being updated. Fig.2 compares the changes of packet delay of those two routing protocols. Compared to the success ratio, the delay is not affected much by the change of the intensity.

The second set of simulation results presents the effect of recurrence interval of radio jamming source. For the simulations, we used fixed values for the intensity and the speed; the intensity was set to 12 m and the speed was 4 m/sec and 2 m/sec. In Fig.3 and Fig.4, AODV 2 and GPSR 2 use the speed of 2 m/sec, and AODV 4 and GPSR 4 use the speed of 4 m/sec. The interval was varied between 50 and 90 seconds.

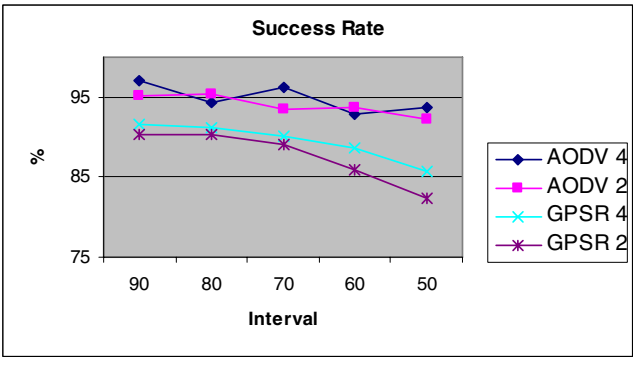

Fig. 3. Success Ratio versus Interval

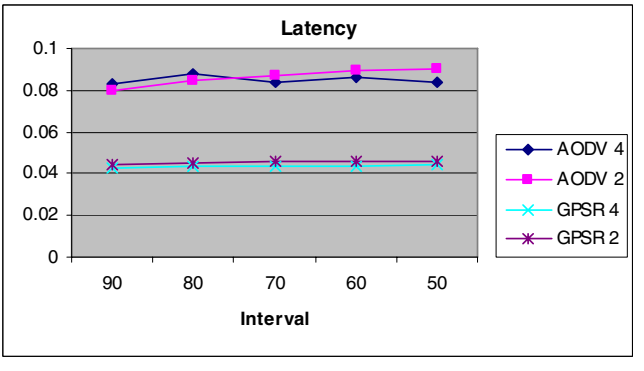

Fig. 4. Delay versus Interval

Fig.3 compares the effect of the recurrence interval on the success ratio between two routing protocols: AODV and GPSR. The x-axis indicates the recurring interval. As described earlier, the recurrence interval indicates how quick the source returns back to the same location. In general, this parameter has a higher value as the size of WSN gets bigger on the assumption that a single radio jamming source was used. As shown in Fig.3, both AODV and GPSR have lower success ratio as the recurrence interval gets shorter. One difference is that GPSR has bigger performance degradation with the increase of the interval. Fig.4 compares the effect of the recurrence interval on the packet delay. The delay is gradually increased as the interval gets shorter.

The third set of simulation results presents the effect of moving speed of radio jamming source. For the simulations, we used fixed values for the intensity and the interval; the intensity was set to 12 m and the interval was 50 and 70 seconds. In Fig.5 and Fig.6, AODV 50 and GPSR 50 use the interval of 50 seconds, and AODV 70 and GPSR 70 use the speed of 70 seconds. The speed was 8, 4, 2, and 1 m/sec.

Fig.5 compares the effect of the speed on the success ratio. The x-axis indicates the moving speed of the mobility radio jamming source. As described earlier, the speed indicates how fast the jamming source moves around in the WSN. As shown in Fig.5,

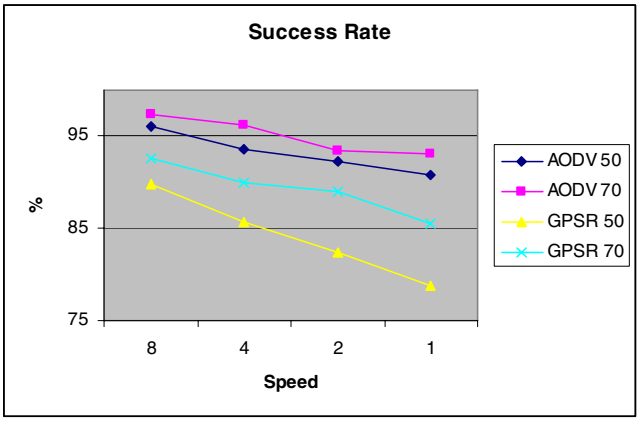

Fig. 5. Success Ratio versus Speed

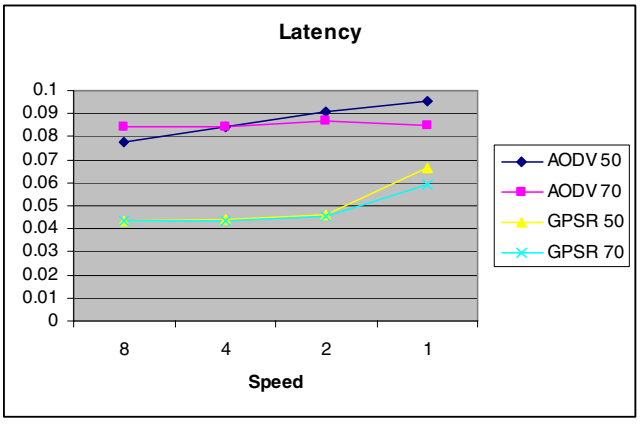

Fig. 6. Delay versus Speed

both AODV and GPSR show steep degradation of success ratio as the speed is increased. Fig.6 presents the effect of the mobility of radio interference on the packet delay. The delay is increased rapidly as the radio jamming source moves faster.

5 Conclusions

We used a simulation method to investigate the effect on mobile radio jamming on the performance of large-scale WSN. The behavioral characteristic of mobility radio jamming attack was modeled with three parameters: interference intensity, recurrence interval, and moving speed. Among the parameters, the speed has the most conspicuous effect on both success ratio and delay. As the speed changes from 8 m/sec to 1 m/sec, the success ratio drops by up to 10 %. On the other hand, the delay increases by up to 55 %.

References

1. Rahul C. Shah, Summit Roy, Sushant Jain, and Waylon Brunette, "Data MULEs: Modeling and Analysis of A Three-tier Architecture for Sparse Sensor Networks," in Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications (SPNA), Anchorage, Alaska, May 2003.
2. Ember, "EM2420 2.4 GHz IEEE 802.15.4/ZigBee RF Transceiver," available at http://www.ember.com/downloads/pdfs/EM2420datasheet.pdf.
3. Crossbow Technology Inc., "Avoiding RF Interference between WiFi and Zigbee," available at http://www.xbow.com.
4. C.E. Perkins and E.M. Royer, "Ad-hoc On Demand Distance Vector Routing," in Proceedings of the WMCSA'99, 1999.
5. Brad Karp and H.T. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks," in Proceedings of the Mobicom, 2000.
6. Qing Fang, Jie Gao, and L.J. Guibas, "Locating and Bypassing Routing Holes in Sensor Networks," in Proceedings of the Infocom, 2004.
7. T.Fuji and S.Nishioka, "Selective Handover for Traffic Balance in Mobile Radio Communications," in Proceedings of the ICC, 1992.
8. Al R. Shah, Hossam Hmimy, and George Yost, "Models and Methodology of Coverage Verification in Cellular Systems," in Proceedings of the IEEE Vehicular Technology Conference, 1998.
9. Liang Qin and Thomas Kunz, "Pro-active Route Maintenance in DSR," ACM SIGMOBILE Mobile Computing and Communication Reviews, Vol 6, No 3, July 2002.
10. Anthony D. Wood and John A. Stankovic, "Denial of Service in Sensor Networks," IEEE Computer, 35:48-56, Oct. 2002.
11. Anthony D. Wood, John A. Stankovic, and Sang H. Son, "JAM: A Jammed-Area Mapping Service for Sensor Networks," in Proceedings of the 24th IEEE International Real Time Systems Symposium, 2003.
12. Nadeem Ahmed, et al., "The Holes Problem in Wireless Sensor Neworks: A Survey," Technical Report, UNSW-CSE-TR-043, the University of South Wales, Sydney, Australia, 2004.
13. NS2 Simulator for 802.1.5.4, available at http://ees2cy.engr.ccny.cuny.edu/zheng/pub/file.
14. Crossbow Technology Inc., "MICAz Wireless Measurement System," available at http://www.xbow.com/Products.
15. Steibeis-Transfer Centre, "Compatibility of IEEE802.15.4 (Zigbee) with IEEE802.11 (WLAN), Bluetooth, and Microwave Ovens in 2.4 GHz ISM-Band," available at http://www.ba-loerrach.de.
16. I. Howit and Jose A. Gutierrez, "IEEE 802.15.4 Low Rate-Wireless Personal Area Network Coexistence," Issues Wireless Communications and Networking, Vol.3, pp. 1481-1486, 2003.
17. I. Howitt, V. Mitter, and J. Gutierrez, "Empirical Study for IEEE 802.11 and Bluetooth Interoperability," in Proceedings of the IEEE Vehicular Technology Conference, Spring 2001.
18. N. Golmie, "Bluetooth Dynamic Scheduling and Interference Mitigation," ACM Mobile Networks, MONET Vol. 9, No. 1, 2004.