© 2017 IJSRSET | Volume 3 | Issue 3 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Security in Wireless Sensor Networks : Data Aggregation

Abhishek Nigam, Saurabh Jaiswal, Neha Agarwal
Department of Computer Science and Engineering, Sri Ramswaroop University, Lucknow, India

ABSTRACT

Recent advances in wireless sensor networks (WSNs) have led to many new promising applications including habitat monitoring and target tracking. However, data communication between nodes consumes a large portion of the total energy consumption of the WSNs. Consequently, Data Aggregation techniques can greatly help to reduce the energy consumption by eliminating redundant data traveling back to the base station. The security issues such as data integrity, confidentiality, and freshness in data aggregation become crucial when the WSN is deployed in a remote or hostile environment where sensors are prone to node failures and compromises. There is currently research potential in securing data aggregation in the WSN. Data-centric technologies are needed that perform in-network aggregation of data to yield energy-efficient dissemination. In this paper we model jamming prevention techniques and compare its performance with traditional prevention techniques. In the proposed work source-destination placement and communication network density on the energy costs and delay associated with data aggregation. In my proposed work, defense strategies offers significant performance gains across a wide range of operational scenarios. The main goal of defense strategies algorithms is to gather and protect jamming areas in an energy efficient manner so that network lifetime is enhanced.

Keywords : Wireless sensor networks, data aggregation, routing protocols, LEACH and SPIN, Jamming

I. INTRODUCTION

In this article we survey issues related to jamming sensor networks by examining both the attack and defend sides of the problem. We present different jamming attack strategies that might be used against sensor networks. Later, we examine methods that can be employed by the sensor network in order to detect the presence of jamming. We illustrate that basic statistics alone (e.g., signal strength) are not sufficient for classifying the presence of a jammer, and more advanced detection methods are needed. We examine two strategies for coping with jamming. The first strategy involves avoiding the jammer in either the spectral or spatial sense, and can be achieved by changing channel allocations or, in mobile sensor networks, by moving nodes away from the jammer. The second strategy involves competing with the jammer by adjusting the transmission power levels and employing error correction in order to have more resilience against jamming. Finally, we present concluding remarks.

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions. A WSN system incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes (see Figure 1). The wireless protocol you select depends on your application requirements. Some of the available standards include 2.4 GHz radios based on either IEEE 802.15.4 or IEEE 802.11 (Wi-Fi) standards or proprietary radios, which are usually 900 MHz.

II. METHODS AND MATERIAL

1. Wireless Sensor Networks Applications

Military Applications

- Monitoring friendly forces, equipment, and ammunition
- Battlefield surveillance
- Reconnaissance of opposing forces and terrain
- Targeting
- Battle damage assessment
- Nuclear, biological, and chemical attack detection

Environmental Applications

- Forest fire detection
- Bio-complexity mapping of environment
- Flood detection
- Precision Agriculture
- Air and water pollution

Health Applications

- Telemonitoring of human physiological data
- Tracking and monitoring doctors and patients inside a hospital
- Drug administration in hospitals

Automotive Applications

- Reduces wiring effects
- Measurements in chambers and rotating parts
- Remote technical inspections
- Conditions monitoring e.g. at a bearing

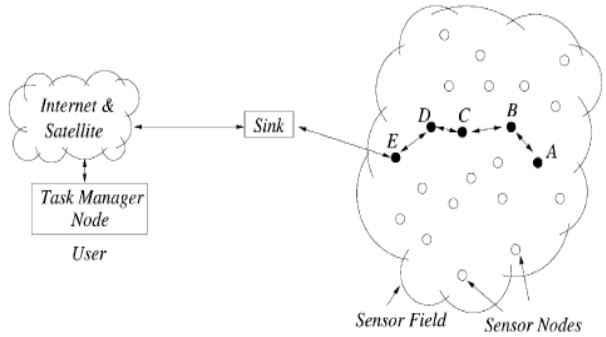

Figure 1: WSN Communication Architecture

Data Aggregation in WSNs

Data coming from multiple sensor nodes are aggregated if they are about the same attribute of the phenomenon when they reach the same routing node on the way back to the sink

- Solves implosion and overlap problem
- Energy efficient

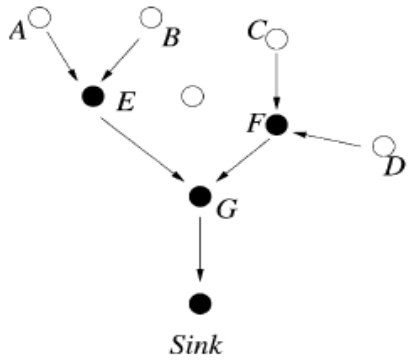

Figure 2 : Data Aggregation in WSNs

2. Jamming Attacks

There are many different attack strategies an adversary can use to jam wireless communications [4–6], While it is impractical to cover all the possible attack models that might exist, in this article we review a wide range of jammers that have proven to be effective.

2.1 Constant Jammer : The constant jammer continually emits a radio signal, and can be implemented using either a waveform generator that continuously sends a radio signal [7] or a normal wireless device that continuously sends out random bits to the channel without following any MAC-layer etiquette [4]. Normally, the underlying MAC protocol allows legitimate nodes to send out packets only if the channel is idle. Thus, a constant jammer can effectively prevent legitimate traffic sources from getting hold of a channel and sending packets.

Deceptive Jammer: Instead of sending out random bits, the deceptive jammer constantly injects regular packets to the channel without any gap between subsequent packet transmissions. As a result, a normal communicator will be deceived into believing there is a legitimate packet and be duped to remain in the receive state. For example, in TinyOS, if a preamble is detected, a node remains in the receive mode, regardless of whether that node has a packet to send or not. Even if a node has packets to send, it cannot switch to the send state because a constant stream of incoming packets will be detected.

Random Jammer: Instead of continuously sending out a radio signal, a random jammer alternates between sleeping and jamming. Specifically, after jamming for a while, it turns off its radio and enters a “sleeping” mode. It will resume jamming after sleeping for some time.

During its jamming phase, it can behave like either a constant jammer or a deceptive jammer. This jammer model tries to take energy conservation into consideration, which is especially important for those jammers that do not have unlimited power supply.

Reactive Jammer: The three models discussed above are active jammers in the sense that they try to block the channel irrespective of the traffic pattern on the channel. Active jammers are usually effective because they keep the channel busy all the time. As we shall see in the following section, these methods are relatively easy to detect. An alternative approach to jamming wireless communication is
to employ a reactive strategy. The reactive jammer stays quiet when the channel is idle, but starts transmitting a radio signal as soon as it senses activity on the channel. One advantage of a reactive jammer is that it is harder to detect.

2.2 Types of jamming attacks

2.2.1 Constant jammers

A constant jammer continuously produces high-power noise that represents random bits. The bit generator does not follow any media

2.2.2 Random jammers

A random jammer operates randomly in both sleep and jam intervals. During sleep interval, it sleeps irrespective of any traffic on the network,
and during jam interval, it acts as a constant or reactive jammer. That jammer does not follow any MAC protocol. The PDR increases when the sleep interval increases and the packet size decreases.

2.2.3 Deceptive jammers

These jammers continuously send illegitimate packets so that the channel appears busy to the legitimate nodes. They are protocol aware and increase carrier sensing time for the legitimate nodes indefinitely. The difference between a deceptive and a constant jammer is that a constant jammer sends random bits continuously while a deceptive jammer sends packets which appear legitimate to the receiver.

2.2.4 Reactive jammers

A reactive jammer activates when it senses the transmission on the channel. If the channel is idle, it remains dormant and keeps sensing the channel. On sensing the transmission, it transmits enough noise resulting some sufficient number of bits corrupted in the legitimate packet so that packet checksum is not recovered by the receiver and the packet is discarded. Hence, it causes the drop in PDR.

2.2.5 Shot noise-based intelligent jammers

Shot noise-based intelligent jammers are protocol-aware jammers that just beat forward error correction (FEC) scheme used at physical and MAC layers [8]. IEEE 802.11b networks use convolutional coding at the physical layer. Single continuous pulse interfering legitimate packet can completely drop it if it is able to beat the FEC scheme used in the packet [7, 9].

2.3 Characterizing jamming attacks

A jamming attack can be detected easily, less effective, energy efficient, or protocol aware. How to characterize a jamming attack? There are a few commonly used metrics characterizing the jamming attacks:

- Least detection probability
- Protocol aware so that they are less likely to detect
- Authentication of users
- Strength against FEC codes
- Strength at physical layer to beat channel coding techniques
- Energy conservation is to get highest jamming efficiency with least energy used

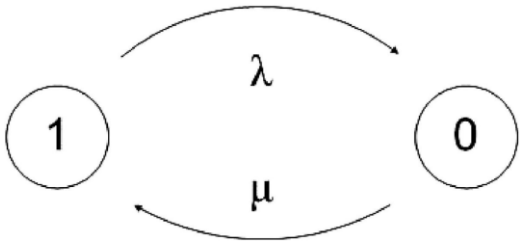

Figure 3: State Transition diagram for tow state random jammer

```
Input: totalPDR(N) = MeasurePDR() : N ∈ Neighbors
Output: Jammer Type Alert
if (totalPDR ≤ threshPDR) then
    ΔS = SampleSignalStrength() -
    NormalSignalStrength()
    PDRSSV = CheckPDRSSVariation(totalPDR,ΔS)
    if (PDRSSV == false) then
        Post NetworkError()
    end
    else
        symbolTT = GetSymbolTransmissionTime()
        packetTT =
        GetPacketTransmissionTime(packetLength)
        PW = GetObservedPulseWidth()
        if (PW ≤ 2 * symbolTT) then
            Post ProtocolAwareIntelligentjammed()
        end
        else if (PW == packetTT) then
            Post ReactiveJammed()
        end
        else if (PW == ConstantJammed()) then
            Post ConstantJamming()
        end
        else if (PW == RandomPulse()) then
            sleepInterval = GetSleepInterval()
            if (sleepInterval > packetTT) then
                totalPDR > 0 else
                    totalPDR == 0
                end
            end
        end
    end
end
```

Algorithm 1: Jammer detection and classification algorithm

3. Advanced Detection Strategies

Mapping Jammed Areas

Following the detection of whether a node is jammed, it is desirable for the network to map out regions of the sensor network that are jammed. By having a map of jammed areas, network services can use this knowledge to influence routing, power management, and higher-layer planning. A protocol for mapping out the jammed regions of a sensor network was presented in [9]. In this article jamming detection is performed by monitoring channel utilization. Once the sensors observe that their channel utility is below a preset threshold, they conclude that they are jammed. Following detection, the jammed nodes bypass their MAC-layer temporarily and broadcast JAMMED messages, announcing the fact that they are jammed. These JAMMED messages will not be able to be received by other jammed neighbors. However, those neighbors on the boundary of the jammed region, but are not themselves jammed themselves, will be able to hear the JAMMED messages, though potentially at a higher error rate. Once non-jammed sensors receive JAMMED messages, they initiate the mapping procedure. These non jammed nodes

exchange and merge information describing which nodes they have witnessed as jammed, where those jammed sensors are located, along with neighbor information. By continuing the exchange of information regarding witnessed jammed nodes, the network will eventually be able to map out the boundary of a jammed area.

III. CONCLUSION

Proposed system will detect Jamming and Replay attack by using minimum energy minimization and furthermore prevention by packet filtering technique. We are decreasing the memory usage for detection of replay attack by using hash procedure. By using hash function, the energy usage is amplified and Performance is improved. Motesec-Aware is an efficient network layer security system also the security is increased by using access control mechanism. Motesec-Aware is ready to achieve to the goals of considerably less energy consumption and higher security than previous works.

This helps to use the proposed implementation on any operating system and for Future work, we can find the actual source of attack from where the replay and jamming attack is happening. Due to the low-cost design of sensor nodes, and the ease with which they may be reprogrammed, sensor networks will be very susceptible to intentional radio interference attacks. This article has surveyed both the attack and defend side of jamming wireless sensor networks. Four different types of jamming devices, which involved bypassing MAC layer carrier sensing, have been discussed. We then turn to the problem of detecting the presence of jamming, where we have illustrated why simple statistics are not sufficient. Multimodal detection methods have recently been proposed as a means to circumvent this challenge. Following detection, it is desirable that the network can repair itself. Toward this end, two evasion strategies have been discussed: the first involving the sensor network adapting its operating frequencies, the second suitable for mobile sensor networks and involving nodes relocating themselves. A different defense strategy involves sensors trying to out-compete the jammer by employing error correcting codes and increasing the node transmission power. Both evasion and competition

strategies are at an early stage of investigation by the community, and as these techniques mature an important area for study will be understanding and classifying the scenarios where one defense strategy is advantageous over another.

IV. REFERENCES

[1]. Xu W, Trappe W, Zhang Y, Wood T: The feasibility of launching and detecting jamming attacks in wireless networks. In Proceedings of the 6th ACM International Symposium on Mobile ad hoc Networking and Computing (MobiHoc 2005). New York,USA; May 2005:46-57.

[2]. Bayrataroglu E, King C, Liu X, Noubir G, Rajaraman R, Thapa B: On the performance of IEEE 802.11 under jamming. In Proceedings of the 27th Conference on Computer Communications(INFOCOM '08). Phoenix AZ, USA; 13–18 Apr 2008.

[3]. Hamieh A, Ben-Othman J: Detection of jamming attacks in wireless Ad Hoc networks using error distribution. In International Conference on Communications (ICC '09). Dresden, Germany; 14–18 Jun 2009:1-6.

[4]. Zou X, Deng J: Detection of fabricated CTS packet attacks in wireless LANs. In Proceedings of the 7th International ICST Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness (QSHINE '10). Houston,USA; 17–19 Nov 2010:105-115.

[5]. Zou X, Deng J: Detecting and mitigating the impact of wideband jammers in IEEE 802.11 WLANS. In Proceeding of the 6thInternational Wireless Communications and Mobile Computing Conference. New York: ACM; 2010:57-61.

[6]. Yu M, Su W, Zhou M: A new approach to detect radio jamming attacks in wireless networks. In International Conference on Networking Sensing and Control. Chicago,USA; 10–12 Apr 2010:721-726.

[7]. Thuente D, Acharya M: Intelligent jamming in wireless networks with applications to 802.11b and other networks. In Proceedings of the IEEE MILCOM IEEE. NJ, USA: Piscataway; 2006:1075-1081.

[8]. Wikipedia . Accessed 23 Jun 2012 http://en.wikipedia.8. org/wiki/Shot Hussain A, Saqib NA: Protocol aware shot-noise based radio frequency jamming method in 802.11 networks. In Proceedings of the 8th International Conference on Wireless and Optical Communications Networks. Paris,France; 24–26 May 2011:1-6.

[9]. Pelechrinis K, Iliofotou M, Krishnamurthy V: Denial of service attacks in wireless networks: the case of jammers. Communications Surveys and Tutorials 2010, 13: 245-257.

Author's Profile

Abhishek Nigam had have completed B.C.A. from BBDNITM (Agra University) in 2009 & my M.C.A. from BBDNITM (UPTU) in 2011. Pursuing M.Tech from Shri Ramswaroop Memorial University (SRMU) Lucknow. Specialization – Computer Science My Area of Interest is Computer Networks and Network Security