ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

Detection and Prevention of Resource Depletion Attacks in Wireless Ad Hoc Sensor Networks

Haseena[1], M.Venkatesh Nayak [2]

Student, Department of CSE, Chiranjeevi Reddy Institute of Technology, Anantapuram, India [1]

HOD, Department of CSE, Chiranjeevi Reddy Institute of Technology, Anantapuram, India[2]

Abstract: Wireless Ad Hoc Sensor Networks are the networks with will collection of wireless devices. They meant for some kind of sensing tasks. There are many real world utilities of these kinds of network. For instance, they are used for environment monitoring, studying wildlife habitat besides a plethora of military and civilian applications. These sensor networks suffer from lack of resources. In other words, they do have fewer resources such as energy. Therefore they are subjected to numerous attacks. Resource depletion attack or vampire attack is one such attack where a compromised node involves in generating more network traffic which depletes energy of the nodes. The vampire node behaves as per the underlying protocol making the network difficult to detect such attack. This is the problem to be addressed. Recently Vasserman and Hopper proposed a method to prevent "vampire attacks" in Ad Hoc Sensor Networks. Their research reveled that vampire attacks are not specific to any protocol. However, they depend on many routing protocols. In this paper we implement a prototype application that simulates the Wireless Ad Hoc Sensor Network with number of nodes and sink with the resource depletion attack model. Our empirical results reveal that the prototype is able to provide encouraging results.

Keywords*:* Wireless networks, denial of service, sensor networks, and resource depletion attacks

I. INTRODUCTION

Wireless Sensor Networks are widely used for various real world applications both in civilian and military purposes. The sensor networks help in sensing data from surroundings and send to base stations or sink. A collection of sensor nodes generate data and send it to the sink in many to one communication. The nodes are expected to cooperate with other nodes in the network for data transmission. In this sense, every node will act as transmitter and receiver. A typical sensor node appears as shown in Figure 1.

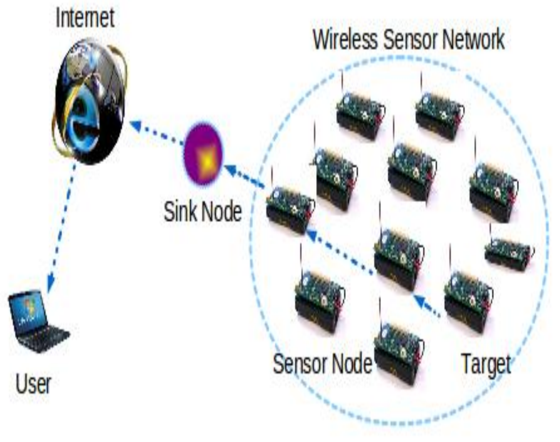


Fig. 1 – Typical wireless sensor network

As can be shown in Figure 1, wireless sensor network is a collection of sensor nodes which can sense data about targets. The sensor nodes sense the unknown object data and send to sink node. The sink node can be accessed by authorized users through Internet. In fact the sink node can be queried in order to monitor the area under coverage of WSN.

In this paper we present a simulation application that demonstrates a typical WSN with collection of nodes sending data sink. The application simulates source node, destination node, sink node and intermediate node. It demonstrates energy depletion attacks and the prevention of such attacks. The remainder of the paper is structured as follows. Section II presents related work. Section III provides the prototype application details. Section IV presents the experimental results while section V concludes the paper.

II. RELATED WORK

Energy depletion attacks are potential problems in WSN. In [1] early mention of power related problems were discussed and named it as "sleep deprivation torture". Another research in [2] takes care of "denial-of-sleep" where attacks are considered at MAC layer. In [3] and 4] experiments are made on resource exhaustion problems at MAC and also transport layers in wireless networks. Malicious circles were described in [5] and [6] for increasing efficiency of MAC layer and corresponding routing protocols.

Depletion of resources is very dangerous in power constrained systems. SYN flood attacks [7] are one of the popular examples for power depletion kind. When power depletion occurs each node gets exhausted with respect to energy and finally switched off. It causes the reduction of network life time. Such attacks can be defeated using cryptographic puzzles as explored in [8], [9] and [10]. These solutions can avoid malicious nodes in wireless networks. As vampire attacks depend on amplification,

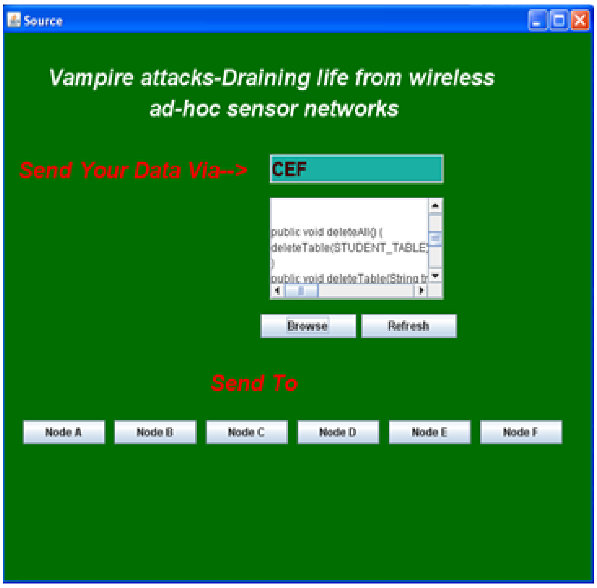
ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

these solutions are not effective to justify a perfect solution.

There are other researches as explore in [11], [12], [13], [14], [15], [16], [17] for attacks and defenses pertaining to QoS and network performance. Transport layer is the main focus of this research where vampires do not drop packets but they cause heavy consumption of energy. Energy depletion attack is the focus of this paper.

III. PROTOTYPE APPLICATION

We built a prototype application that simulates the Wireless Sensor Network environment and demonstrates malicious attacks that can cause resource depletion in the network. These attacks lead to the reduction of network life time.

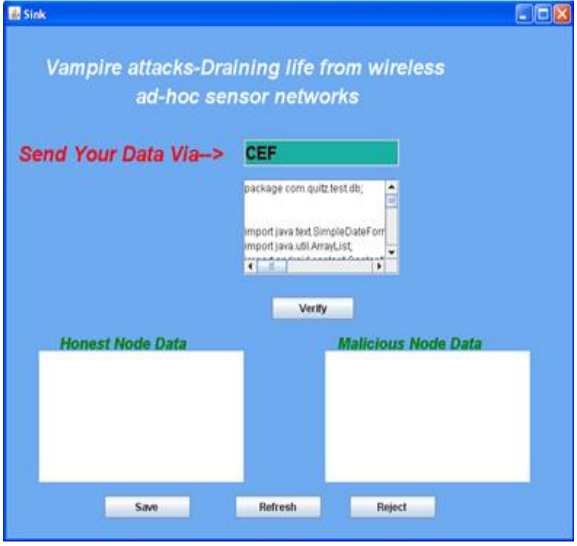


Send Your Data Via--> CEF

```
public void deleteAll() {
deleteTable(STUDENT_TABLE);
}
public void deleteTable(String tr
```

Figure 3 – UI for source node

As can be seen in figure 3, it is evident that the prototype application has provision for simulating the source node which sends data to destination node. The data is transmitted to destination through intermediary nodes.



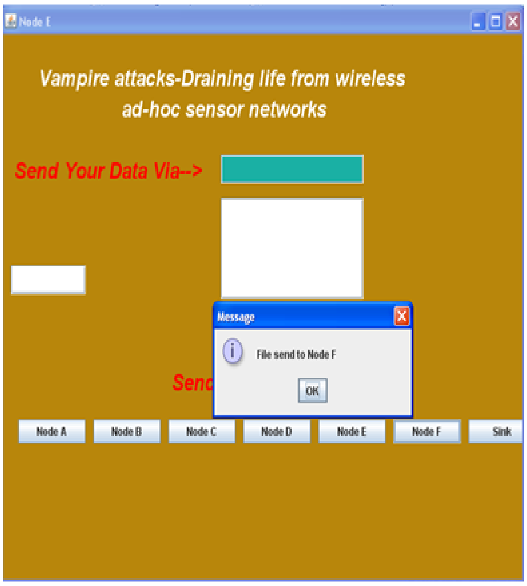
Send Your Data Via--> CEF

```
package com.quitz.test.db;


import java.text.SimpleDateForm
import java.util.ArrayList;
```

Figure 4 – UI for sink

As can be seen in Figure 4, it is evident that the sink node functionality is simulated here. It is able to provide honest and malicious nodes data besides eliminating such attack by rejecting them. The sink node is supposed to get data from sensor nodes.



File send to Node F

Figure 5 – UI for an intermediary node that can forward data to destination

As can be seen in Figure 5, it is evident that the intermediate node is capable of sending data to destination through other nodes possible in the middle.

IV. EXPERIMENTAL RESULTS

Experiments are made with the prototype application where the simulation is made to obtain statistics of the attack model. The results are obtained in terms of faction of total nodes versus fraction of node energy consumed.

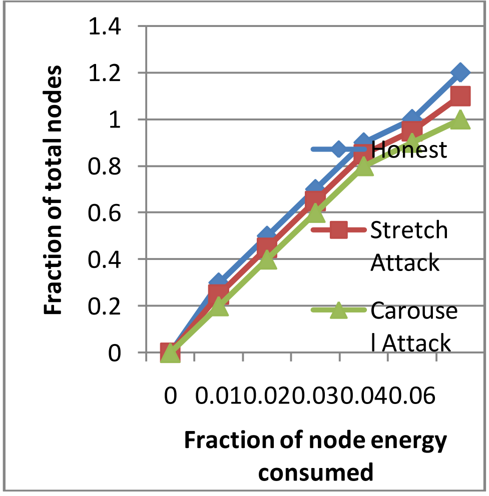


Figure 1 – Node energy distribution under various attack models

As can be seen in Figure 1, it is evident that the energy consumption of the stretch attack is more than that of carousel attack. The honest scenario exhibits least energy consumption that is the normal scenario.

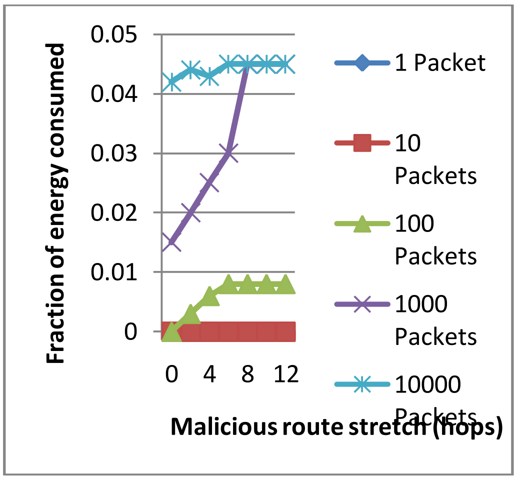


Figure 2 – Energy consumption against stretch attack

When malicious nodes transferring various numbers of packets with long paths built artificially, the fraction of energy consumed is plotted. The results revealed that with more number of packets and hops, the energy consumption is more.

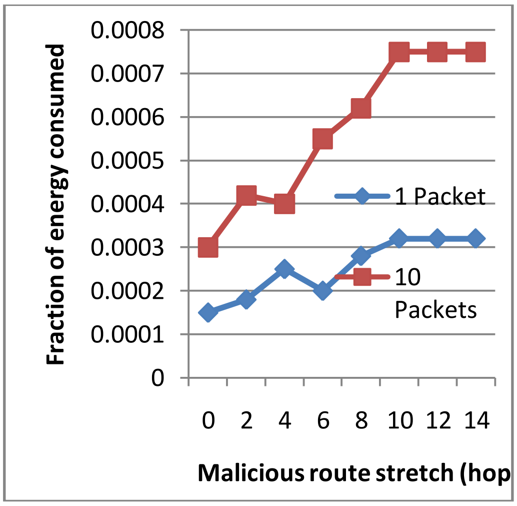


Figure 3 – Malicious route stretch versus energy consumption

As can be seen in Figure 3, it is evident that the energy consumption is more with number of packets more and hops are more with respect to the fraction of energy consumed.

V. CONCLUSION AND FUTURE WORK

In this paper we studied energy draining attacks in Wireless Ad Hoc Sensor networks. Since the sensor networks are resource constrained, they are vulnerable to various attacks. Especially the energy depletion attack is devastating. The vampire node, the node which has been compromised, behaves as per the underlying protocol making the network difficult to detect such attack. Since the vampire node sends protocol compliant messages, it is possible that the other nodes believe the messages as genuine and try to answer them. In this process lot of unnecessary messaging takes place. This causes other nodes to lose energy resources and finally switched off. This way all nodes are gradually coming out of network and the network life span gets decreased drastically This is one of the potential attacks in the network that cause maximum damage and the purpose of deploying such network is defeated. To overcome this problem we built a solution in this paper and that is demonstrates through a prototype, a custom simulator, built using Java programming language. The simulation results reveal that such attacks can be prevented and this will help in real time implementation of a protocol to prevent attacks. In future we intend to work on the similar kind of attacks in other wireless networks.

REFERENCES

[1] F. Stajano and R. Anderson, “The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks,” Proc. Int’l Workshop Security Protocols, 1999.

[2] D.R. Raymond, R.C. Marchany, M.I. Brownfield, and S.F. Midkiff, “Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols,” IEEE Trans. Vehicular Technology, vol. 58, no. 1, pp. 367-380, Jan. 2009.

[3] D.R. Raymond and S.F. Midkiff, “Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses,” IEEE Pervasive Computing, vol. 7, no. 1, pp. 74-81, Jan.-Mar. 2008.

[4] A.D. Wood and J.A. Stankovic, “Denial of Service in Sensor Networks,” Computer, vol. 35, no. 10, pp. 54-62, Oct. 2002.

[5] H. Chan and A. Perrig, “Security and Privacy in Sensor Networks,” Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.

[6] B. Parno, M. Luk, E. Gaustad, and A. Perrig, “Secure Sensor Network Routing: A Clean-Slate Approach,” CoNEXT: Proc. ACM CoNEXT Conf., 2006.

[7] D.J. Bernstein, “Syn Cookies,” http://cr.yp.to/syncookies.html, 1996.

[8] T. Aura, “Dos-Resistant Authentication with Client Puzzles,” Proc. Int’l Workshop Security Protocols, 2001.

[9] T.J. McNevin, J.-M. Park, and R. Marchany, “pTCP: A Client Puzzle Protocol for Defending Against Resource Exhaustion Denial of Service Attacks,” Technical Report TR-ECE-04-10, Dept. of Electrical and Computer Eng., Virginia Tech, 2004.

[10] L. von Ahn, M. Blum, N.J. Hopper, and J. Langford, “CAPTCHA: Using Hard AI Problems for Security,” Proc. 22nd Int’l Conf. Theory and Applications of Cryptographic Techniques (Eurocrypt), 2003.

[11] S. Goldberg, D. Xiao, E. Tromer, B. Barak, and J. Rexford, “Path-Quality Monitoring in the Presence of Adversaries,” Proc. ACM SIGMETRICS Int’l Conf. Measurement and Modeling of Computer Systems, 2008.

[12] M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang, “Reduction of Quality (RoQ) Attacks on Internet End-Systems,” Proc. IEEE INFOCOM, 2005.

[13] A. Kuzmanovic and E.W. Knightly, “Low-Rate TCP-Targeted Denial of Service Attacks: The Shrew vs. the Mice and Elephants,” Proc. SIGCOMM, 2003.

[14] Y.-K. Kwok, R. Tripathi, Y. Chen, and K. Hwang, “HAWK: Halting Anomalies with Weighted Choking to Rescue Well-Behaved TCP Sessions from Shrew DDoS Attacks,” Proc. Int’l Conf. Networking and Mobile Computing, 2005.

[15] X. Luo and R.K.C. Chang, “On a New Class of Pulsing Denial-of-Service Attacks and the Defense,” Proc. Network and Distributed System Security Symp. (NDSS), 2005.

[16] H. Sun, J.C.S. Lui, and D.K.Y. Yau, “Defending against Low-Rate TCP Attacks: Dynamic Detection and Protection,” Proc. IEEE 12th Int’l Conf. Network Protocols (ICNP), 2004.

[17] G. Yang, M. Gerla, and M.Y. Sanadidi, “Defense Against Low-Rate TCP-Targeted Denial-of-Service Attacks,” Proc. Ninth Int’l Symp. Computers and Comm. (ISCC), 2004.