Research Paper Engineering

Enhancing Energy Efficiency by Detecting and Protecting from Vampire Attack in Wireless Sensor Networks

Abdul Razak Qureshi Department of Computer Science & Engineering, Rajiv Gandhi College of Engineering, Research & Technology, Chandrapur-442401(MS)

Prof. R.K. Krishna Department of Electronics, Rajiv Gandhi College of Engineering, Research & Technology, Chandrapur-442401 (MS)

ABSTRACT

a wireless sensor networks (WSN) can be defined as a network of small embedded devices called sensors which communicate wirelessly with ad-hoc configuration. This paper explores permanent energy depletion attack at routing protocol layer in network, which causes disable infected node from network permanently by draining battery power. This Vampire attacks are not specific to the routing protocol layer, but rather rely on the properties of classes of routing protocol. These attacks are easy to carry out and difficult to detect by sending protocol compliant messages. We analyse and compare such attack and energy consumption in AODV routing protocol

KEYWORDS Vampire attack, Wireless Sensor Network attack, WSN, Clustering, Node, Routing.

I. Introduction

Wireless sensors are small tiny embedded devices with low memory, low computing power and low battery life. Various applications such as continuous connectivity, weather monitoring, industry and instantly -deployable communication for first responders and military. These networks already consider environmental conditions, factory performance, and troop deployment, to name some applications. [1][2] WSN it's functioning towards the people and industry is bulky so the reasons behind it -lack of availability of network, lost productivity, power outages, environmental destructions, and even lost lives. So to mitigate such problems there are methods which can stop attacks from happening on the short-term availability of a network but they do not address attacks that affect long term availability — the most permanent denial of service attack is to completely drain energy of node. These attacks are different from previously-seen DoS , reduction of quality (RoQ), and routing infrastructure attacks as they do not disrupt immediate availability of node in network, but work over time to completely disable a network called vampire attack.[4][5]

Vampire attacks are not protocol-specific and they do not depend on design properties or implementation faults of specific routing protocols, but rather exploit properties of protocol classes such as link state, distance-vector, source routing, and geo-graphic and beacon routing. [2][3][4][5]Vampire attacks do not depend on flooding the network with large amounts of data rather try to transmit as little data as possible to get the largest energy drain which prevents a rate limiting solution. Vampires attack use protocol compliant messages which make it very hard to detect and prevent in network. [7] Evaluate the vulnerabilities of existing protocols to routing layer battery reduction attacks. Existing work on secure routing attempts to confirm that intruder cannot cause path discovery to return an invalid network path, but Vampires do not modify discovered paths instead of that it uses existing valid network paths and protocol compliant messages. [4][6].

Vampire attackers are malicious insider node having the same resources and level of network access as honest nodes. Attacker location within the network is assumed to be fixed and random. This is far from the strongest adversary model; rather this configuration represents the average expected damage from Vampire attacks. [6][7] Smart adversary placement or dynamic node compromise would make attacks far more damaging. In this paper we are exploring energy consumption in AODV routing protocol before and after Vampire attack and how to enhance the energy of node and protect from vampire attack will consider future enhancement work.

II. Simulation setup

We conducted series of simulation to analyse AODV routing protocol using NS2 simulator and compare before and after Vampire attack using delay in packet delivery, energy consumption, and throughput. Following are the requirements for simulation

Software requirement: Vamware Workstation ver 8, Fedora 2.6,

Simulator: NS2 ver 2.34

Language: TCL and Awk scripting

Parameters used to generate Wireless sensor network (WSN) in NS2 simulator.

Routing protocol	AODV
Number of Nodes	35
Topology dimension	670m X 670m
Traffic Type	CBR
MAC Type	802.11 MAC Layer
Packet Size	512 Bytes
Antenna Type	Omni Dimension

Table 1: Parameters for NS2 Simulator

Methodology

1. Install NS2 simulator and configure the path for the execution
2. Create initial WSN setup using above parameters and assuming node energy level is high
3. Execute tcl file and analyse the NAM animator for delay graph and Energy consumption
4. Repeat step 3 and analyse the output
5. Implement vampire attack and execute tcl file
6. Analyse delay graph and energy consumption after vampire attack in Wireless Sensor network
7. Repeat step 5 and analyse output
8. Compare packet delay and energy consumption for pre

and post vampire attack

III. Simulation Results and Comparison

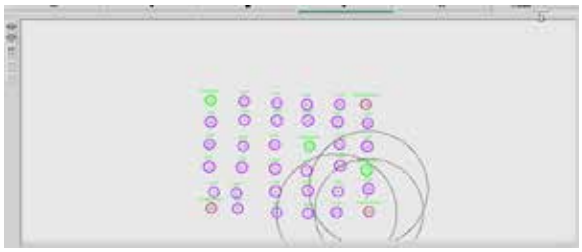


Fig1: WSN Setup showing Communicator and node

Fig 1 shows wireless sensor network setup including data transmission initiated between communicator and nodes

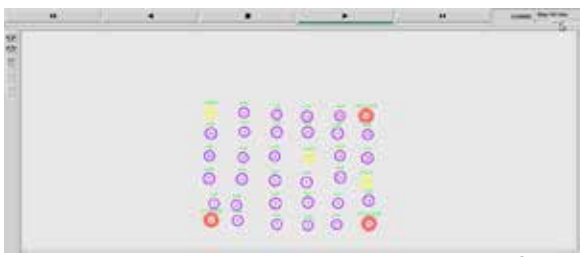


Fig2: WSN setup with Vampire attackers and infected nodes

Fig 3 shows number of vampire attack (33, 34, 35) and infected node (30, 31, 32) in wireless sensor network

Packet Transmission Delay

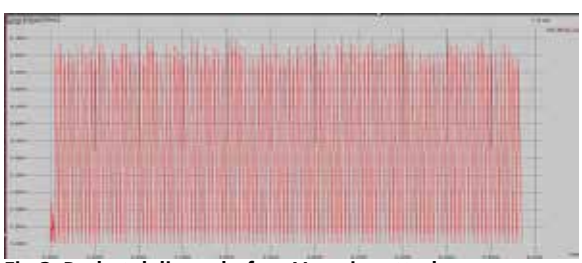


Fig 3: Packet delivery before Vampire attack

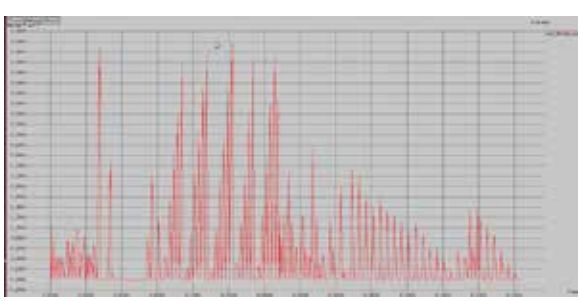


Fig4: Packet delay post Vampire attack

As shown in figure 4, which has more packet transmission delay due to keep sending data to various nodes in WSN as compare to fig 4 .

Energy Comparison

Energy consumes whenever some nodes sends data to other node/base station in WSN. The fig 6 clearly shows that energy consumption is more after vampire attack as compare to before attack in WSN (Fig 5) using AODV routing protocol scenario. Attacker node keep sending protocol compliant messages to nodes, which required more energy for communications among nodes and attacker. Whereas less energy consumes in normal communication i.e without attack.

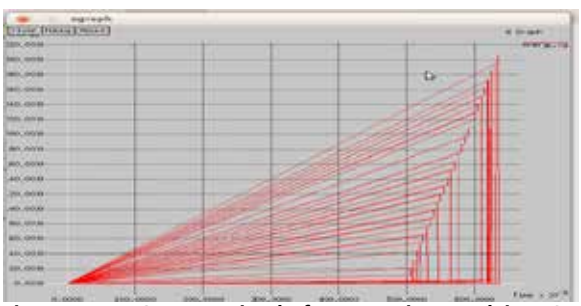


Fig 5: Energy Consumption before Vampire attack in WSN

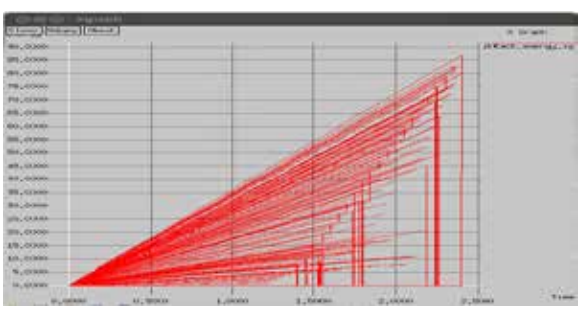


Fig 6: Energy consumption after Vampire attack in WSN

IV. Conclusions

Thus we have studied AODV routing protocol energy consumption before and after vampire attack using NS2 simulator.

The energy consumption is more after vampire attack which may disable the wireless sensor network permanently. How to enhance node energy efficiency and protecting from Vampire attack by implementing LEACH protocol is left for future work by author.

Acknowledgment

We would like to thanks Department of Computer Science & Engineering and Department of Electronics, RCERT Chandrapur (MS), India, for providing infrastructure and guidance to understand attacks in Wireless sensor networks, Wireless communications.

REFERENCES

[1] Eugene Y. Vasserman and Nicholas Hopper "Vampire attacks: draining life from wireless ad-hoc sensor networks," | IEEE Trans on mobile computing vol.12 no.2 year 2013 | | [2] LinaR.Deshmukh and Amol D. Potgantwar "Prevention of vampire attacks in WSN using Routing Loop," | proceedings of IRF International conference, 5th & 6th Feb 2014, Pune India | | [3] Susan Sharon George and Suma R "Attack-Resistant Routing for Wireless Ad Hoc Networks," International Journal | of CS & IT, vol.5. (3), 2014 | | [4] A.Vincy, and V.Uma Devi "Maximizing Lifetime of Nodes in Wireless Ad Hoc Sensor Network by preventing | Vampire Attack," IEEE International Conference on Innovations in Engineering and Technology, 21st& 22nd Mar 2014 | | [5] Gowthami.M, and Jessy Nirmal.A.G "Mitigating Vampire Attack in Wireless Ad-Hoc Sensor Networks", IJARCST | 2014 Vol. 2. Jan-Mar 2014 | | [6] Vidya. M and Reshmi.S "Contending Against Energy Debilitating Attacks in Wireless Ad Hoc Sensor Networks", | IJIRAE vol. 1. Mar 2014 | | [7] Soram Rakesh Singh and Narendra Babu C R "Improving the Performance of Energy Attack Detection in WSN by | Secure Forward Mechanism", International Journal of Scientific and Research Publications, Vol 4, July 2014 | | [8] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, Ariadne: A secure on-demand routing protocol for ad hoc networks, MobiCom, 2002. | | [9] Anoopa S et al Int. Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 4, Issue 4(Version 6), April 2014, pp.01-07