International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Issue 5, Volume 2 (May 2015) www.ijirae.com

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— Wireless sensor networks are ad-hoc low power sensor node has more research in computing directions and denial of communications at routing levels. This paper explores energy draining attack at routing protocol layer, which permanently disable node from network 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 difficult to detect and easy to carry out by sending protocol compliant messages. We discuss methods to mitigate this type of attack and have proposed the techniques for enhancing energy of nodes.

Keywords— Vampire attack, Wireless Sensor Network attack, WSN, Clustering, Node, Routing.

I. INTRODUCTION

In future ad-hoc wireless sensor networks (WSNs) will present exciting new applications, such as on demand computing power, continuous connectivity 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] Now-a day's WSN become more popular but 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 overcome these we can use the wireless ad-hoc network.[2][3] These methods 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 disrupt battery life of node. This system also consider how routing protocols lack security from vampire attacks since they drain the life from nodes in the networks. These attacks are different from previously-seen DoS , reduction of quality (RoQ), and routing infrastructure attacks as they do not disrupt immediate availability, but work over time to completely disable a network.[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. These attacks are very hard to detect and prevent because Vampires use protocol compliant messages. [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].

All routing protocols employ at least one topology discovery period. Our attackers are malicious insiders 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. While for the rest of the project will assume that a node is permanently disabled once its battery power is exhausted, consider nodes that recharge their batteries in the place, using either continuous charging or switching between active and recharge cycles. In case of continuous charging, power draining attacks would be effective only if the adversary is able to consume power at least as fast as nodes can recharge.[7] Considering that packet processing drains at least as much energy from the victims as from the attacker, a continuously recharging adversary can keep at least one node permanently disabled at the cost of its own functionality.

II. BRIEF LITERATURE SURVEY

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

Ad-hoc low-power wireless networks are an exciting research direction in sensing and pervasive computing. Prior security work in this area has focused primarily on denial of communication at the routing or medium access control levels.

In this explores resource depletion attacks at the routing protocol layer, which permanently disable networks by quickly draining nodes' battery power. These "Vampire" attacks are not specific to any specific protocol, but rather rely on the properties of many popular classes of routing protocols. [1]

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

In sensing and pervasive computing ad-hoc low-power wireless networks are an exciting research. Prior security work has first focused on denial of communication at the routing or levels of media access control. We find that all examined protocols are affected to Vampire attacks, which are destructing, hard to detect, and are easy to carry out using as few as one malicious insider sending only protocol compliant messages. In case of worst case, a single Vampire can increase network-wide energy usage by a factor of O (N), where N in the number of nodes of network. [2]

Susan Sharon George and Suma R "Attack-Resistant Routing for Wireless Ad Hoc Networks," International Journal of CS & IT, vol.5. (3), 2014

A number of security services: availability, confidentiality, authentication, integrity and non-repudiation are crucial to ensure a reliable data transfer over such networks and to secure the network resources. Prior security work in this area has concentrated primarily on the DoS attack at the routing layer. This paper focuses on a more devastating, difficult to prevent, and easy to carry out attack called Vampire attacks, which quickly drain nodes' battery power leading to the permanent disabling of nodes. This paper discusses methods to mitigate these types of attacks, by introducing a new protocol that limits the damage caused by Vampire attacks. [3]

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

There are a lot of protocols developed to protect from DOS attack, but it is not completely possible. One such DOS attack is Vampire attack-Draining of node life from wireless ad-hoc sensor networks. This explores resource depletion attacks at the routing protocol layer, which permanently disable networks by quickly draining nodes' battery power. .In this phase detecting and preventing denial of service attack based on secret sharing (SS) algorithm and increasing network lifetime based on switching the node states. [4]

Gowthami.M, and Jessy Nirmal.A.G "Mitigating Vampire Attack in Wireless Ad-Hoc Sensor Networks", IJARCST 2014 Vol. 2. Jan-Mar 2014

Ad-hoc sensor network and routing data in them is a most significant research area. There are lots of protocols established to protect from DOS attack, but it is not perfectly possible. This project illustrates a technique to tolerate the attack by employing the Cluster Head. In case of each Vampire attack, the Cluster Head employs in this situation and distributes the packet to destination without dropping the packet. Thus give a successful and reliable message delivery even in case of Vampire attack. [5]

Vidya. M and Reshmi.S "Contending Against Energy Debilitating Attacks in Wireless Ad Hoc Sensor Networks'', IJIRAE vol. 1. Mar 2014

In this we explores resource exhausting attacks at the routing protocol layer, which disable networks permanently by quickly draining node's battery power. These attacks are not protocol specific, but rather rely on the class properties of routing protocols. Here we find that all examined protocols are vulnerable to Vampire attacks are easy to carry out using as few as one malicious node inside sending only protocol-compliant messages. [6]

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

Wireless ad-hoc sensor networks and routing data in them is a significant research area. The objective of this paper is to examine resource depletion attacks at the routing protocol layer, which attempts to permanently disable network nodes by quickly draining their battery power. This type of attack is called as vampire attack. Methods to detect and secure data packets from vampires during the packet forwarding phase is discussed. PLGP with attestations (PLGP-a) is used for identifying malicious attack. [7]

III. PROBLEM FORMULATION

All routing protocols employ at least one topology discovery period, since ad hoc deployment implies no prior position knowledge. Consider immutable but dynamically organized topologies. Differentiate between on-demand routing protocols, where topology discovery is done at transmission time, and static protocols, where topology is discovered during an initial setup phase, with periodic rediscovery to handle rare topology changes. Adversaries are malicious insiders and have the same resources and level of network access as honest nodes. Adversary location within the network is assumed to be fixed and random. Assume that a node is permanently disabled once its battery power is exhausted.

Source routing protocols: malicious packet source can specify paths through the network which are far longer than optimal, wasting energy at intermediate nodes who forward the packet based on the included source route.

Routing schemes: where forwarding decisions are made independently by each node directional antenna and wormhole attacks can be used to deliver packets to multiple remote network positions, forcing packet processing at nodes that would not normally receive that packet at all, and thus increasing network-wide energy expenditure.

Route and topology discovery phases: if discovery messages are flooded, an adversary can, for the cost of a single packet, consume energy at every node in the network.

IV. OBJECTIVE

Following are the objectives to overcome the problem formulation:

1. To evaluate the vulnerabilities of existing protocols.
2. To routing layer battery depletion attacks.
3. To modify an existing sensor network routing protocol to provably bound the damage from Vampire attacks during packet forwarding.
4. To transmit little data with largest energy drain.
5. A fully satisfactory solution for Vampire attacks during the topology discovery phase, but suggested some intuition about damage limitations possible with further modifications

V. PROPOSED METHODOLOGY

In this section we are proposing the methodology to increase the energy efficiency of node and protection from Vampire attack. For increasing energy efficiency of node, we are using a protocol i.e. **LEACH protocol**. LEACH is single-hop clustering routing protocol in WSN. In LEACH protocol, all nodes forms a clusters which is self-organised, each cluster has one cluster head and other non-cluster nodes. Using balancing node energy consumption, it selects cluster head randomly and each node has an equal chance to be cluster head. [7]

VI. CONCLUSIONS

Thus we have studied various attack and have also proposed the protocol used to improve efficiency of node and protecting from vampire attack. Therefore the proposed technique is an effective approach to improve energy efficiency of node and protect from Vampire attack.

ACKNOWLEDGMENT

We would like to thanks Department of Computer Science & Engineering, RCERT Chandpur for providing infrastructure and guidance to understand attacks in Wireless sensor networks.

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

