Volume 5, Issue 5, May 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Survey on Vampire Attacks in Wireless Ad-Hoc Sensor Networks

Meghana N
M. tech (persuing)
Department of Computer Science &Engg
VTU Department Of PG Studies, Mysuru, India

Dr. G. F. Ali Ahammed
Associate Professor
Department of Computer Science &Engg
VTU Department Of PG Studies, Mysuru, India

Abstract-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. This paper 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. We find that all examined protocols are susceptible to Vampire attacks, which are devastating, difficult to detect, and are easy to carry out using as few as one malicious insider sending only protocol compliant messages. In the worst case, a single Vampire can increase network-wide energy usage by a factor of O(N), where N in the number of network nodes. We discuss methods to mitigate these types of attacks, including a new proof-of-concept protocol that provably bounds the damage caused by Vampires during the packet forwarding phase.

***Index Terms—Denial of service, security, routing, ad-hoc networks, sensor networks, wireless networks*.**

I. INTRODUCTION

Ad-hoc wireless sensor networks (WSNs) promise exciting new applications in the near future, such as ubiquitous on-demand computing power, continuous connectivity and instantly-deployable communication for military and first responders. Such networks already monitor environmental conditions, factory performance, and troop deployment, to name a few applications. As WSNs become more and more crucial to the everyday functioning of people and organizations, availability faults become less tolerable — lack of availability can make the difference between business as usual and lost productivity, power outages, environmental disasters, and even lost lives; thus high availability of these networks is a critical property, and should hold even under malicious conditions. Due to their ad-hoc organization, wireless ad-hoc networks are particularly vulnerable to denial of service (DoS) attacks, and a great deal of research has been done to enhance survivability.

II. LITERATURE REVIEW

Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly, mainly focuses on the design and study DoS attacks in order to assess the damage that difficult-to-detect attackers can cause. The authors presented a novel DoS attack perpetrated by JellyFish: relay nodes that stealthily disorder, delay, or periodically drop packets that they are expected to forward, in a way that leads astray end-to-end congestion control protocols. This attack is protocol- compliant and yet has a devastating impact on the throughput of closed-loop flows, such as TCP flows and congestion-controlled UDP flows.

Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig introduce a secure routing protocol for Ad-hoc wireless networks. The deployment of sensor networks in security-and safety-critical environments requires secure communication primitives. In this study, the authors design, implement, and evaluate a new secure routing protocol for sensor networks.

Jae-Hwan Chang and Lindros Tassiulas had extended the maximum lifetime routing problem to include the energy consumption at the receivers during reception. In wireless sensor networks where nodes operate on limited battery energy, the efficient utilization of the energy is very important.

III. EXISTING SYSTEM

Existing work on secure routing attempts to ensure that adversaries cannot cause path discovery to return an invalid network path, but Vampires do not disrupt or alter discovered paths, instead using existing valid network paths and protocol compliant messages. Protocols that maximize power efficiency are also inappropriate, since they rely on cooperative node behavior and cannot optimize out malicious action.

IV. PROPOSED SYSTEM

In proposed system we show simulation results quantifying the performance of several representative protocols in the presence of a single Vampire. Then, we modify an existing sensor network routing protocol to provably bound the damage from Vampire attacks during packet forwarding.

V. METHODOLOGY

In this paper, a layered approach is used to solve the problem with the vampire attacks. Vampire packet (malicious packet) monitoring is performed both in network layer (routing protocol layer) and application layer. The network layer checking helps to point out the vampire packets from the network and the application layer checking helps to find out the vampires inside the running processes (ie, inside the node). Whenever an incoming packet is detected that is a vampire then the packet will not be forwarded and it will be discarded. Whenever a vampire is detected inside the node simply we can eliminate it.

A clean-slate secure sensor network routing protocol[2] by Parno, Luk, Gaustad, and Perrig "PLGP" can be modified to provably resist Vampire attacks during the packet forwarding phase. The original version of the protocol, although designed for security, is vulnerable to Vampire attacks. PLGP consists of a topology discovery phase, followed by a packet forwarding phase, with the former optionally repeated on a fixed schedule to ensure that topology information stays current. Here a modification in the forwarding phase of PLGP to provably avoid the above-mentioned attacks. First check the no backtracking property, satisfied for a given packet if and only if it consistently makes progress toward its destination in the logical network address space. More formally: No-backtracking is satisfied if every packet p traverses the same number of hops whether or not an adversary is present in the network.

To preserve no-backtracking, need to add a verifiable path history to every PLGP packet. The resulting protocol, PLGP with attestations (PLGPa) uses this packet history together with PLGP's tree routing structure so every node can securely verify progress, preventing any significant adversarial influence on the path taken by any packet which traverses at least one honest node. Whenever a node n forwards packet p,this by attaching a non-repayable attestation (signature). These signatures form a chain attached to every packet, allowing any node receiving it to validate its path. Every forwarding node verifies the attestation chain to ensure that the packet has never travelled away from its destination in the logical address space.

A. System Architecture

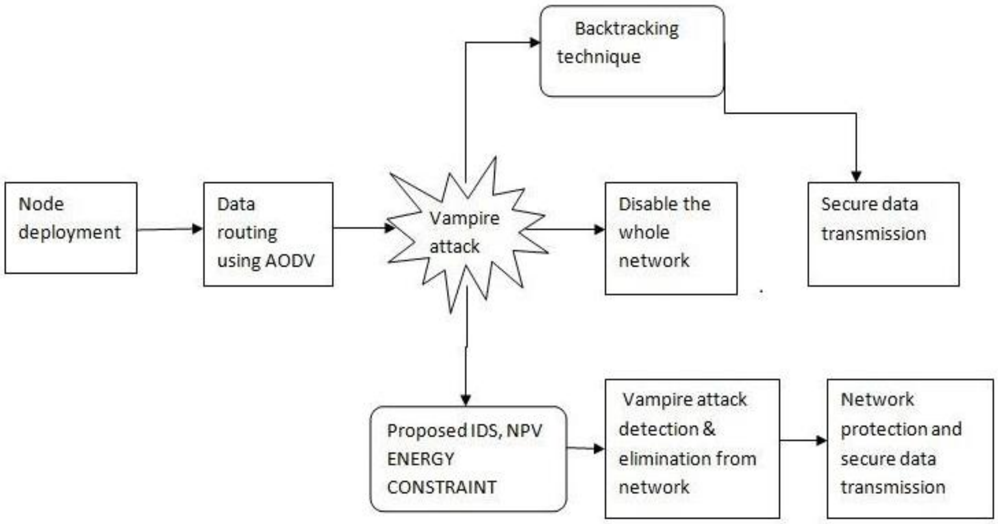
Backtracking technique
Node deployment
Data routing using AODV
Vampire attack
Disable the whole network
Secure data transmission
Proposed IDS, NPV ENERGY CONSTRAINT
Vampire attack detection & elimination from network
Network protection and secure data transmission

Fig1. Block Diagram

B. Module Description

1) Node Configuration Setting: The mobile nodes are designed and configured dynamically, designed to employ across the network, the nodes are set according to the X, Y, Z dimension, which the nodes have the direct transmission range to all other nodes.

2) Data Routing: The source and destination are set at larger distance, the source transmits the data packets to destination through the intermediate hop nodes using UDP user data gram protocol, link state routing like PLGP act as an ad hoc routing protocol.

3) Vampire Attack*;* The malicious node enters the network, and affects the one of the intermediate node by sending false packets. So the malicious node drain the energy of the intermediate node, the intermediate energy level goes to 0 joules. So the data transmission is affected, the path tends to be failure between source and destination. As a result source retransmits the data in another path to destination. If the vampire attack continues it will disable the whole network.

4) Backtracking Technique: The back tracking technique is used to identify legitimate nodes in the particular path. The nodes accept the data only after the execution of back tracking technique. If source transmits the data to next neighbor node, the next node verifies the source identity using back tracking process. Through this technique the data is transmitted securely in the presence of vampire nodes.

5) Intrusion Detection System: The energy constraint IDS is used to detect the malicious nodes from the network, for that purpose the energy level for all nodes are calculated after every data iteration process. Maximum nodes have an average energy level in certain range, due to the nature of vampire nodes have a abnormal energy level like malicious node energy level is three times more than the average energy level, by this technique the malicious nodes can be identified easily.

6) Malicious Node Elimination: After the IDS process the malicious nodes detected. The TA trusted authority informs to all nodes in the network and eliminate the malicious node from the network. So by eliminating malicious node we can form a secure network.

7) Graph Examination: The performance analysis of the existing and proposed work is examined graphical analysis.

VI. CONCLUSION

We defined Vampire attacks, a new class of resource consumption attacks that use routing protocols to permanently disable ad-hoc wireless sensor networks by depleting nodes' battery power. These attacks do not depend on particular protocols or implementations, but rather expose vulnerabilities in a number of popular protocol classes. We showed a number of proof-of-concept attacks against representative examples of existing routing protocols using a small number of weak adversaries, and measured their attack success on a randomly-generated topology of 30 nodes.

ACKNOWLEDGEMENT

We would like to thank all the people involved in research related in vampire attack in wireless sensor network & I like to thank my guide Dr. G.F. Ali Ahammed, Associate Professor, Computer Science & Engineering Department.

REFERENCES

[1] E Y Vasserman, N Hopper, Vampire Attacks: Draining life from wireless Ad hoc sensor networks, IEEE Transactions on Mobile Computing, volume 12, issue 2, published on feb 2013(pages 318-332)

[2] Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig, Secure sensor network routing: A clean-slate approach, CoNEXT, 2006.

[3] INSENS: Intrusion-tolerant routing for wireless sensor networks, Computer Communications 29 (2006), no. 2.

[4] Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly, Denial of service resilience in ad hoc networks, MobiCom, 2004.

[5] Gergely Acs, Levente Buttyan, and Istvan Vajda, Provably secure on demand source routing in mobile ad hoc networks, IEEE Transactions on Mobile Computing 05 (2006), no. 11.

[6] Jae-Hwan Chang and Leandros Tassiulas, Maximum lifetime routing in wireless sensor networks, IEEE/ACM Transactions on Networking 12 (2004), no. 4.