IJDCST @June-July-2015, Issue- V-3, I-5, SW-06
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Protocol Level Proven Methods to mitigate the Vampire Attacks on Wireless Sensor Networks

[#1]Avula Srikanth, [#2]R.V.Kishore Kumar
[#1]srikanthavula9@gmail.com, [#2]rejeti.kishore@gmail.com
[#1]M.Tech Student, Sri Mittapalli college of Engg
[#2]Assistant Professor, Dept of CSE, Sri Mittapalli college of Engg

Abstract: Low configured wireless PDA's become a part of human life in the format of mobiles, sensors, cameras and other small digital electronic components. Due to the mobility and on-demand connectivity security is the major concern in this area always. Former researches on this area were concerned only on secured communications, medium access control levels. Apart from the general attacks at protocol level and data access level, recently PDA's encountered the problems of "Vampire Attacks" which damage the system by draining the batteries quickly. Our analysis revealed that all existing protocols are facing the problems from these vampire attacks, which are cumbersome to identify and resolve. In this paper we concentrates on this Vampire attacks and we proposed the new methods to resist the vampire attacks successfully on these low configured PDA devices. The proof of concept of these techniques was proven that our proposed methods will resist the vampire attacks successfully.

Keywords: Vampire attacks, protocol security, routing, ad-hoc networking.

I. Introduction

With advent of Ad hoc wireless sensor networks and its relevant applications, we can expect the drastic improvements in real life applications like dynamic power receiving, longer connectivity with failures, auto configurable network deployment and high speed communications etc. As WSN's required to accomplish day to day human needs either business or personal needs, we should design them more robust, unbreakable and more secured. There are plenty of emergency applications (military applications, disaster management applications, medical applications etc.) are using these WSN's, so it is our responsibility to concern on them to improvise to give the better services to its clients.

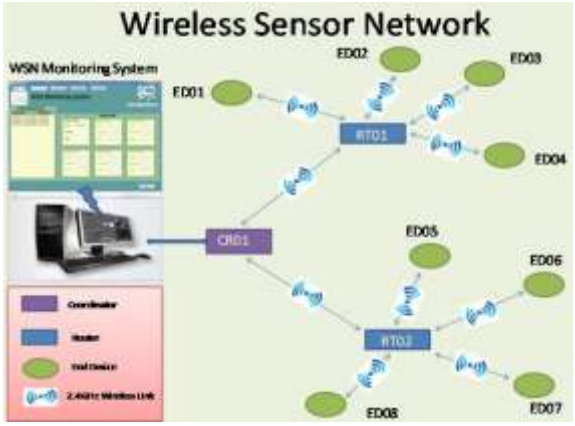


Figure1. The Basic Deployment of WSN's Block Diagram

Figure1 represents the basic architecture of wireless sensor networks with root system, monitoring system, deployed nodes, coordinating nodes and 2.4 GHZ wireless links ets. In general the most frequent

problems of these applications are power outages, security issues, communicational errors, less available resources, external threats (on either hardware / software) etc. Most of the recent past researches on these technologies were concerned on the common issues [1] of WSN's like protocol attacks, routing attacks, communication attacks, data tampering attacks and authentication attacks etc.

Since a decade, in the area of wireless sensor networks a new kind of attacks was introduced by adversaries are "Vampire Attacks" [2]. Instead of concentrating on breaking security and tampering the data, Vampire Attacks will drain the battery of node which cause to lose the connectivity frequently. These attacks are distinct from previously-studied DoS [2 and 5], reduction of quality (RoQ), and routing infrastructure attacks as they do not disrupt immediate availability, but rather work over time to entirely disable a network. While some of the individual attacks are simple, and power-draining and resource exhaustion attacks have been discussed before, prior work has been mostly confined to other levels of the protocol stack, e.g. medium access control (MAC) or application layers, and to our knowledge there is little discussion, and no thorough analysis or mitigation, of routing-layer resource exhaustion [5 and 6] attacks.

The major contributions of this research are:

- Vulnerabilities identification on existing WSN routing protocols
- Evaluating the root causes and showcase of Vampire attacks effect on protocols performance
- Upgrading the protocols to resist from vampire attacks

Experiments on our proposed methodologies and its results are showing that, our methodologies are having the better performance over data transfer and resisting the vampire attacks.

II. Literature Review

In this section we discuss about various types of vampire attacks on WSN's and their effect on damaging the node communication capability in detail. The main aim of the vampire attacks is draining the battery and reducing the life time of connectivity by insisting some malfunction background processes in running.

A) SYN Flood Attack:

This attack exploits an implementation characteristic of the *Transmission Control Protocol* (TCP), and can be used to make server processes incapable of answering a legitimate client application's requests for new TCP connections [7]. Any service that binds to and listens on a TCP socket is potentially vulnerable to TCP SYN flooding attacks. Because this includes popular server applications for e-mail, Web, and file storage services, understanding and knowing how to protect against these attacks is a critical part of practical network engineering.

The attack has been well-known for a decade, and variations of it are still seen. Although effective techniques exist to combat SYN flooding, no single standard remedy for TCP implementations has emerged. Varied solutions can be found among current operating systems and equipment, with

differing implications for both the applications and networks under defense. This article describes the attack and why it works, and follows with an overview and assessment of the current tactics that are used in both end hosts and network devices to combat SYN flooding attacks.

B) Wormhole Attack:

Wormhole attack is one of the Denial-of-Service attacks [8] effective on the network layer, that can affect network routing, data aggregation and location based wireless security. [3] The wormhole attack may be launched by a single or a pair of collaborating nodes. In commonly found two ended wormhole, one end overhears the packets and forwards them through the tunnel to the other end, where the packets are replayed to local area. In case when they only forward all the packets without altering the content, they are helping the network to accomplish transmission faster. But in majority of the cases, it either drops or selectively forwards the packets, leading to the network disruption. Wormhole attack does not require MAC protocol information as well as it is immune to cryptographic techniques. This makes it very difficult to detect.

III. Mitigating Vampire Attacks on Wireless Sensor Networks

In this section we discuss about our proposed methods to mitigate the vampire attacks and their effect on wireless sensor networks (WSN's). In order to adopt our methods on WSN's sake we had considered the protocol is PLGP [4]. We selected this protocol for our experiments sake, because of the frequent utilization of this on WSN's in almost 60% of applications.

The path diverse problem is the major issue in PLGP as the packets of this protocol don't about the transferring path, which allows the adversaries to divert the path to drop packets. Sometimes this problem even allows the attackers to add and send the malicious packets to the specified destination. This loop makes the PLGP to make vulnerable against Vampire attacks. Due to the limitation of honest nodes to destination only carrying address and identity of packets, there is a chance to insert the malicious nodes by tapping the information of honest nodes. If this process was happened as a flood, all these packets should transfer through various hops of the networks, which may consume the lot of bandwidth and consumes the power of intermediate nodes also.

To resist from the vampire attacks on PLGP, we updated the data packet forwarding procedure in PLGP to mitigate and alleviate the Vampire attacks. No-Back tracing property of our method will recognize the honest packet node and the adversary attack node (malicious node) is used to separate them and drops the malicious nodes if they appeared. The nature of this feature is "No-backtracking is satisfied if every packet p traverses the same number of hops whether or not an adversary is present in the network". This does not imply that every packet in the network must travel the same number of hops regardless of source or destination, but rather that a packet sent to node D by a malicious node at location L will traverse the same number of hops as a packet sent to D by a node at location L that is honest. If we think of this in terms of protocol execution traces, no-

backtracking implies that for each packet in the trace, the number of intermediate honest nodes traversed by the packet between source and destination is independent of the actions of malicious nodes.

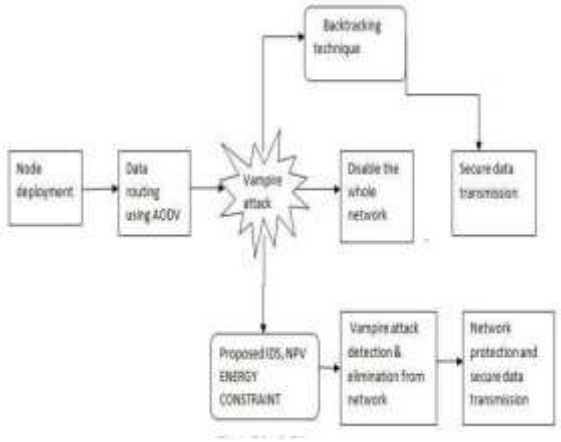


Figure1. Proposed Architecture to Resist from Vampire Attacks

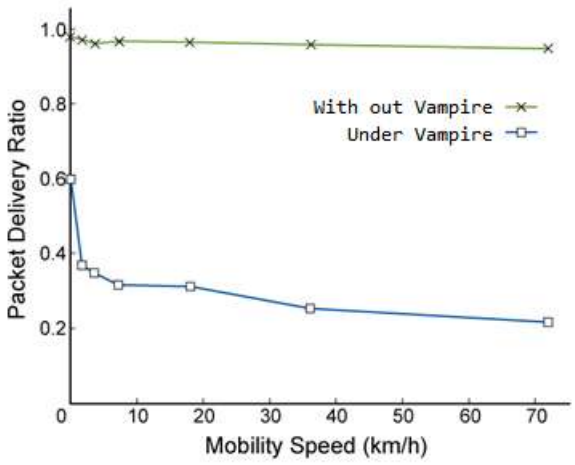
The vampire attack can be prevented entirely by having forwarding nodes check source routes for loops. While this adds extra forwarding logic and thus more overhead, we can expect the gain to be worthwhile in in malicious environments. When a loop is detected, the source route could be corrected and the packet sent on, but one of the attractive features of source routing is that the route can itself be signed by the source. Therefore, it is better to simply drop the packet, especially considering that the sending node is likely malicious. An alternate solution is to alter how intermediate nodes process the source route. To forward a message, a node must determine the next hop by locating itself in the source route. If a node searches for itself from the destination backward instead from the source forward, any loop that includes the current node will be automatically truncated.

IV. Experimental Results

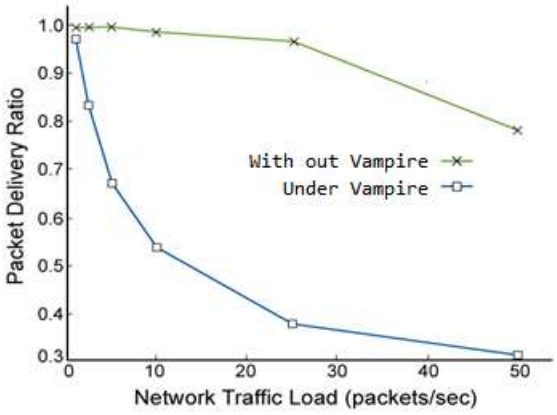
To evaluate the efficiency of proposed methods, we did the experiments with our approach and compared the results against the existing PLGP routing Technology. Experimental results are simulated with NS2 tool and Cygwin combination to obtain the results comparison.

The proposed solution allows sensor nodes to forward RREP packet provided some conditions are met. This gets accomplished by spending additional time and energy. An upper limit can also be placed on waiting time for Probe_Ack messages that is also decided using simulation.

Before forwarding the RREP packet, each node broadcasts Probe message and waits for Probe_Ack message from the two-hop neighbor nodes. Based on the decision taken from the received tag values, decision for forwarding RREP is taken. These additional steps add total transmission time in receiving the RREP packet as well as the energy consumed by the nodes as shown in below graphs Gaprh 1 and Graph2 in detail.



Graph1 Packet Delivery Ratio comparison with mobility speed



Graph2 Packet Delivery Ratio comparison with network traffic load

From these two graphs it is very clear that our proposed techniques are mitigating the effect of Vampire attacks on WSNs.

V. Conclusion

Since a decade, in the area of wireless sensor networks a new kind of attacks was introduced by adversaries are "Vampire Attacks". Instead of concentrating on breaking security and tampering the data, Vampire Attacks will drain the battery of node which causes to lose the connectivity frequently. In this paper we concentrates on this Vampire attacks and we proposed the new methods to resist the vampire attacks successfully on these low configured PDA devices. The proof of concept of these techniques was proven that our proposed methods will resist the vampire attacks successfully.

VI. References

1) Gergely Acs, Levente Buttyan, and Istvan Vajda, Provably secure ondemand source routing in mobile ad hoc networks, IEEE Transactions on Mobile Computing 05 (2006), no. 11.
2) Tuomas Aura, Dos-resistant authentication with client puzzles, International workshop on security protocols, 2001.
3) 3) Saurabh Gupta, SubratKar and S Dharmaraja, "WHOP: Wormhole Attack Detection Protocol using Hound Packet", in International Conference of Innovations in Information Technology, pp. 226 to 231, 2011.\
4) 4) Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig, Secure sensor network routing: A clean-slate approach, CoNEXT, 2006.
5) Zhu, S., Setia, S., and Jajodia, S., "LEAP: Efficient security mechanisms for large-scale distributed sensor Networks", in Proceedings of the 10th ACM Conference on Computer and communications Security, CCS '03. ACM, New York, NY, pp. 62–72, 2003.
6) Asis Nasipuri and Samir R. Das, On-demand multipath routing for mobile ad hoc networks, International conference on computer communications and networks, 1999.
7) David R. Raymond, Randy C. Marchany, Michael I. Brownfield, and Scott F. Midkiff, Effects of denial-of-sleep attacks on wireless sensor network MAC protocols, IEEE Transactions on Vehicular Technology 58 (2009), no. 1.
8) Haibin Sun, John C. S. Lui, and David K. Y. Yau, Defending against low-rate TCP attacks: dynamic detection and protection, ICNP, 2004.