SECURE AND EFFICIENT ROUTING PROTOCOL FOR PREVENTING VAMPIRE ATTACKS IN WIRELESS AD HOC NETWORKS

[1]*Mr.M. Madhangiri., M C A., M.Phil.,*
Assistant Professor, Department of Computer Science,
NGM College, Pollachi, Tamilnadu, India.

[2] *Mr. P. Balamuthukumar., MCA., M.Phil., SET.,*
Assistant Professor, Department of Computer Science,
Hindusthan College of Science and Commerce, Ingur, Perundurai, Tamilnadu, 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), wherein 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.

Keywords: Sensor Networks, Wireless Networks, Ad-hoc Networks, Routing Protocols, Energy consumption, Routing, Security.

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. Vampire attacks are not protocol-specific, in that they do not rely on design properties or implementation faults of particular routing protocols, but rather exploit general properties of protocol classes such as link-state, distance vector, source routing and geographic and beacon routing. Beyond the established technologies such as mobile phones and WLAN, new approaches to wireless communication are emerging; one of them are so called ad hoc and sensor networks. Ad hoc and sensor networks are formed by autonomous nodes. Communicating via radio without any additional backbone infrastructure. A Wireless Sensor Network (WSN) can be defined as a network of small embedded devices, called sensors, which

communicate wirelessly following an ad hoc configuration. They are located strategically inside a physical medium and are able to interact with it in order to measure physical parameters from the environment and provide the sensed information. The nodes mainly use a broadcast communication and the network topology can change constantly due, for example, to the fact that nodes are prone to fail. Because of this, we should keep in mind that nodes should be autonomous and, frequently, they will be disregarded.

1.1 Wireless Ad-hoc Network

An ad-hoc wireless network is a collection of wireless mobile nodes that self-configure to form a network without the aid of any established infrastructure, as shown in without an inherent infrastructure, the mobiles handle the necessary control and networking tasks by themselves, generally through the use of distributed control algorithms. Multi hop connections, whereby intermediate nodes send the packets toward their final destination, are supported to allow for efficient wireless communication between parties that are relatively far apart. Ad hoc wireless networks are highly appealing for many reasons. They can be rapidly deployed and reconfigured. They can be tailored to specific applications, as implied by Oxford's definition. They are also highly robust due to their distributed nature, node redundancy, and the lack of single points of failure. The sensor nodes in

the wireless sensor networks are usually mainly depending on the battery power. To saving the power of nodes must be used a number of techniques. In the one cause of energy loss in wireless sensor network node in the idle consumption, when the nodes are not participating in the processing of transmitting receiving any information but listening and waiting for information from other nodes. There also an energy loss because of packet collusion, where all packets ate involved in the collision are discarded and must be retransmitted. A third cause of energy loss is repeating the process of receiving and transmitting the same packets as a periodically these can be seen as protocol overhead. Vampire attacks based on protocol compliant messages so, it's much detected and prevent. The vampire attacks do not able to address that attacks long-term availability.

2. Existing System

2.1 Routing Packets

The process of routing is done and initialized by the source node. The source node composes the route and transmitting the packet as mentioned route. The packet is forwarding each and every hops towards the destination. A vampire attacks as a composition and transmission of message this impact causes more energy to be consumed by the network that as well as the honest node transmitted a message of the identical amount to the same destination. Even though it's using the different packet headers. The energy wastage of the transmitting and receiving packets in the network while the malicious node present is higher compare the all honest nodes forwarding the packets to the appropriate destination.

2.2 Problem Description

Vampire attack happens in the network in the sense, any of the nodes in the network which is affected or infected and this nodes behavior is abruptly changing for the network behavior, this kind of nodes are called "Malicious node". If malicious nodes present in the network energ that have been using by each and every nodes will increases drastically. The malicious nodes has been place in the network uniquely. First In between the routing nodes, and thesecond placed in the Source node itself. The chance of placing a malicious node in the routing path this makes causing damage in network. Source node identifying the particular packets and selected packets are identified for the routing to the destination. The routing path is discovering by source node by using shortest path routing algorithm and the path shouldn't be changeable by the intermediate nodes. In this type of occasion there is a chance to happening attack. The adversary composes packets with purposely introduced routing loops. This is one of the major problem of the network where the consuming energy of each and every nodes in the network will increasing. Since it sends packets in circle, that shown in the.it targets source routing protocols by exploiting the limited verification of message heads at forwarding nodes, allowing single packets to repeatedly traverse the same set of nodes.

3. Related Work

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. In this section we discuss various protocols proposed for security of wireless sensor networks by different researchers.SNEP protocol was designed as basic component of another protocol SPINS (Security protocol for wireless Sensor Networks) that was basically designed for secure key distribution in wireless sensor networks. SNEP define the primitives for authentication of sensor node, data confidentiality and data integrity. However the drawback of this protocol is lower data freshness. SNEP protocol uses shared counter for semantic confidentiality not initial vectors.Using SNEP the plain text is ciphered with CTR encryption algorithm. Both sender and receivers are responsible to update the shared counter once when they sent or receive cipher blocks. Therefore sending counter in message is not important, however every message has message authentication code (MAC). This is computed from cipher data with the help of CBC-MAC algorithm. When the receiver node receives data it recomputed MAC and compared with the received MAC. *REWARD*

(a) Carousel attack:

- Adversary composes packets with purposely introduced routing loops.
- Sends packets in circles.
- Targets source routing protocols by

exploiting the limited verification of message headers at forwarding nodes, allowing a single packet to repeatedly traverse the same set of nodes.

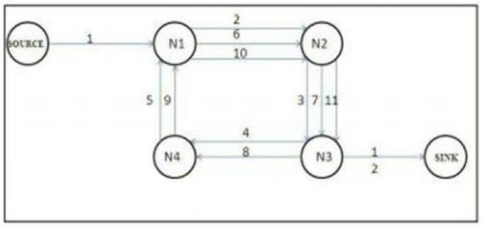

Fig: 2 Carousel attack

(b) Stretch attack:

- An adversary constructs artificially long routes, potentially traversing every node in the network
- Increases packet path lengths, causing packets to be processed by a number of nodes that is independent of hop count along the shortest path between the adversary and packet destination.

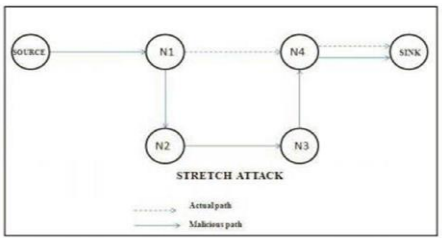

Fig. 3 Stretch attack

3.1 Energy weighted monitoring algorithm to detect vampire attacks

This section focuses on the design details of our proposed protocol EWMA. Where energy of a node gets to threshold level it plays a vital role by performing energy intensive tasks there by bringing out the energy efficiency of the sensors and rendering the network endurable. This pattern based on the energy levels of the sensors.

EWMA functions two phases namely.

1. Network configuring phase
2. Communication phase

1. Network configuring phase

The goal of this phase is to establish a optimal routing path from source to destination in the network. The key factors considered are balancing the load of the nodes and minimization of energy consumption for data communication. In this phase the node with threshold level energy (attacked node) sends ENG_WEG message to all its surrounding nodes. After receiving the ENG_WEG packets the surrounding nodes sends the ENG_REP message that encapsulates information regarding their geographical position and current energy level.

2. Communication Phase:

The main job of communication phase is to avoid the same data packets transmitting through the same node repeatedly to deplete the batteries fastly and leads to network death because of vampire attacks. The process of repeating the packets is eliminated by aggregating the data transmitting within the forwarding node and route the remaining packets safely to the destination. The data aggregation is achieved by first copying the content of thepacket that is transmitting through the node.

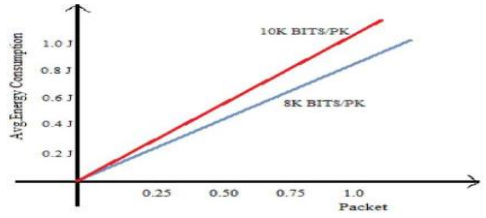

Fig 5. Average Energy Consumption for varying message length

packet size is 10kbits/packet. That is when the message length is increased the average energy consumption of the sensor network is more. This is quite obvious because of greater overhead involved in aggregating and transmitting a larger sized packet or message. A message length of 8kbits/packet as lesser length message may not be in a position to carry out the desired task and a larger length may unnecessary contribute to addition overhead which can degrade the performance of the network.

3.1.1 Individual Energy Consumption in the network:

The individual energy consumption in the network that is the energy consumption of each node is shown in the analysis graph. Totally it is a network of 50 nodes .In the observation it is clear that energy consumption of every node is different. Intially all nodes have the intial energy of 85J. But after network

intialisation the node whose energy drains very fastly is attacked with vampire.

3.1.2 Average path length comparison: Shows Average path length comparison of EWMA path length with attacked or malicious path length. In the figure from the observation it is clear that Attacked path length takes a Hop count of approximately 150 but with EWMA it takes only a hop count of 60 for network size of50 nodes that is a malicious path takes 150 hops for a message to reach it. Destination but with EWMA we can transfer with 60 hops to reach the destination. From the analysis of we can easily understood how much energy is consumed to transfer a packet with 150 hops and with 60 hops. The 150 hops takes more energy and delay than the packet travels with 60 hops.

3.1.3 Effect of adverse nodes on the network:

In the fit clearly shows the effect of adverse nodes on the normal nodes. The analysis shows that if a node is malicious it will cause to death of nodes that is the nodes alive are rapidly decreased. As increase in the number of malicious nodes there is increase in the death of normal nodes. But With EWMA we can increase rate of nodes alive. It is clearly understand that if 5 nodes are affected with vampire it will approximately cause to death of 75 percent of nodes. EWMA concept greatly avoids the death of normal nodes only here are two or three nodes for the overall sensor network. Thus EWMA Concept increases overall lifespan of network by energy efficient routing paths.

4. Protocol and technique for overcoming vampire attacks

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.

Clean-Slate Sensor Network Routing:

- PLGP: a clean-slate secure sensor network routing protocol by Parno et al.
- The original version of the protocol is vulnerable to Vampire attacks.
- PLGP consists of a topology discovery phase, foll owed by a packet forwarding phase.

.

4.1 Data-Verification

In data verification module, receiver verifies the path. Suppose data come with malicious node means placed in malicious packet. Otherwise data placed in honest packet. This way user verifies the data's.

4.2 Denial of service

In computing, a denial-of-service attack or distributed denial-of-service attack is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

4.3 User Module

In user module, verify user and any time create a new path. In security purpose user give the wrong details means display wrong node path otherwise display correct node path.

4.4 Attack Module

Stretch attack, where a malicious node constructs artificially long source routes, causing packets to traverse a larger than optimal number of nodes. An honest source would select the route Source → N1→ N4 → Sink, affecting four nodes including itself, but the malicious node selects a longer route, affecting all nodes in the network. These routes cause nodes that do not lie along the honest route to consume energy by forwarding packets they would not receive in honest scenarios.

4.5 Optimal energy Boost-up protocol (OEBP)

This predicts the vampire attacks based on the existing behavior and finds optimal path optimal topology discovery. Schedules the energy consumption and need of energy if any node performs.

5. Proposed System for Overcoming Vampire attacks

5.1 Ad hoc On Demand Distance Vector Routing Protocol

AODV belongs to the class of Distance Vector Routing Protocols (DV). In a DV every node knows its neighbour's and the costs to reach them. A node maintains its own routing table, storing all nodes in the network, the distance and the next hop to them. If a node is not reachable the distance to it is set to infinity. Every node sends its neighbour's periodically its whole routing table. So they can check if there is a useful route to another node using

this neighbour as next hop. When a link breaks a Count-To-Infinity could happen. AODV is an 'on demand routing protocol' with small delay. That means that routes are only established when needed to reduce traffic overhead. AODV supports Unicast, Broadcast and Multicast without any further protocols. The Count-To-Infinity and loop problem is solved with sequence numbers and the registration of the costs. In AODV every hop has the constant cost of one. The routes age very quickly in order to accommodate the movement of the mobile nodes. Link breakages can locally be repaired very efficiently. To characterize the AODV with the five criteria used by Keshav AODV is distributed, hop-by-hop, deterministic, single path and state dependent.

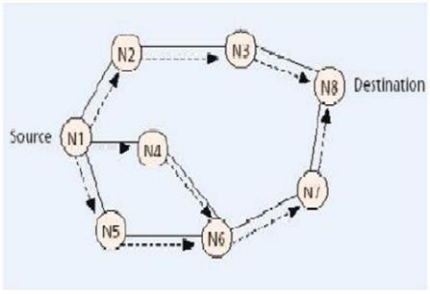

Fig 8. Ad hoc On Demand Distance Vector Routing

5.2 Destination Sequenced Distance Vector

DSDV routing is one of the properties of the ad-hoc network routing protocol. It is a table driven in the type of proactive based protocol routing scheme. Here using two types of routing algorithms one is

1).Link-state algorithm and

2).Distance vectorrouting algorithm.

6. Conclusion

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. Here depending on the location of the adversary, network energy expenditure during the forwarding phase increases drastically. Theoretical worst case energy usage can increase by as much as a factor of O (N) per adversary per packet, where N is the network size. The sensor network routing protocol that provably bounds damage from Vampire attacks by verifying that packets consistently make progress toward their destinations. We have not offered a fully satisfactory solution for Vampire attacks during the topology discovery phase, but suggested some intuition about damage limitations possible. The proposed technique routing protocol are provably bounds damage from Vampire attacks by verifying that packets consistently make progress toward their destinations and reduce the reimbursement.A number of proof of- concept attacks were shown against representative examples of existing routing protocols using small number of weak adversaries, and measured their attack success on a randomly generated topology of 30 nodes. Simulation results show that depending on the location of the adversary, network energy expenditure during the forwarding phase increases from between 50 to 1,000percent.

7. References

[1] Eugene Y. Vasserman and Nicholas Hopper " Vampi re Attacks: Draining Life from Wireless Ad Hoc Sensor Networks " Transactions On Mobile Computing, vol. 12,no. 2, pp.315-332 February 2013

[2] "The Network Simulator - ns-2," http://www.isi .edu/nsnam/ns,2012.

[3] L.M. Feeney, "An Energy Consumption Model for P erformance Analysis of Routing Protocols forMobile Ad Hoc Networks,"Mobile Networks and Applications, vol . 6, no. 3, pp. 239-249, 2001.

[4] Johnson. D.B. Maltz. D.A. and Broch. J. "DSR: T he Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networking, Addison-Wesley,2001

[5] G. Acs, L. Buttyan, and I. Vajda, "Provably Sec ure On-Demand Source Routing in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing.

[6]

AN EFFICIENT KNOWLEDGE OF BIG DATA PROCESSING &TECHNIQUES

Dr. (Mrs) T. Shanmugavadivu MCA., Ph.D.,
Assistant Professor, Department of CS (SF),
NGM College, Pollachi, Tamilnadu, India..
Ms.JeevaShanthini MCA.,
Assistant Professor, Department of CS (SF),
NGM College, Pollachi, Tamilnadu, India.

Abstact

A huge repository of terabytes of data is generated each day from modern information systems and digital technologies such as Internet of Things and cloud computing .Analysis of these massive at a requires a lot of efforts at multiple levels to extract knowledge for decision making. Therefore, big data analysis is a current area of research and development. This high speed growing data is unstructured in the form of blogs, posts , tweets , news articles, video , audio etc. This all is termed as Big Data. Big data is said to bethe massive volume of information that is difficult to be processed using traditional database techniques. Big data can be of both types structured or unstructured. The growth of big data is not stoppable due to social network**.**

Keywords—Big data analytics; Hadoop; Massive data; Structured data; Unstructured Data

I] Introduction:

Big Data are high volume, high velocity, or high-variety data that requires unique forms of processing to enable enhanced decision making, insight discovery, and process optimization

The term 'big data' is explain itself − a collection of large data sets that normal computing techniques cannot process. The term not only refers to the data, but also to the various frameworks, tools, and techniques involved. Technological advancement and the usage of new channels of communication like social networking and new, stronger devices have presented a challenge to industry that we have to find other ways to handle this large volume of data. All this big data is useful when processed. All this data analysis in meaning manner can provide a greater insight and can help in better decision making. The big data has features shown in Figure 1 which makes in different and complex for processing.

II] Types of Big Data Analysis

1. Descriptive Analytics

This summarizes past data into a form that people can easily read. This helps in creating reports, like a revenue, profit and loss statements, sales report, and so on. Also, it helps in the matrix formation of social media data.

2. Diagnostic Analytics

This type of analysis is done to understand the reason that caused a problem. Techniques like drill-down approach, deep data mining ,and data recovery are examples. Organizations use diagnostic analytics because they provide an in-depth insight into a particular problem.

An marketing and product based company report shows that their sales have gone down, although customers are adding products to their carts. This can be due to various reasons like the form didn't load correctly, the shipping fee is too high, or there are not enough payment options available. This is where you can use diagnostic analytics to find the reason.

3. Predictive Analytics

This type of analytics sees into the historical and current data to make predictions of the future. Predictive analytics uses data mining, AI, and