IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

Detection Evaluation and Protection of Vampire Attacks in Ad-Hoc Wireless Sensor Network

Kalyani S Kumar

Dept of ISE, GSSSIETW, Mysuru

Abstract: Wireless Sensor Networks (WSNs) in today's world are the means of communication. These contain nodes that act as transmitter and receivers are prone to different attacks leading to different types of losses. The resource depletion attack that is called vampire attack drains out the energy from the nodes leaving them useless. These attacks are protocol compliant, they are easy to implement. Since they are orthogonal in nature they can easily intrude into any routing protocol. They affect the entire network causing large loss of energy and A vampire attack is caused by the malicious node on the decentralized ad hoc wireless network. The paper analyses how protocols faces these attacks. Vampire attacks are not protocol specific rather uses its compliant message. The current security measures to prevent these attacks are been reviewed along with result of simulation of representative protocols in the presence of a vampire attack is been presented. The paper also describes how the existing sensor network protocol is been modified for protection from the vampire attacks for which PLGP) solution is also been proposed.

Keywords: Wireless Sensor Network; Denial of service; Resource depletion; Routing; Energy consumption; Security; carousel attack; stretch attack; PLGP;

I. INTRODUCTION

Ad hoc wireless sensor network consists of various sensors that are expanded in a space where each sensor performs signal processing and data networking providing operational efficiency. The ad hoc wireless servers are self-organized and energy constrained. These sensor networks are used to detect information of enemy base, monitor environmental changes and are also used for security purposes in various places like shopping and parking area and when these networks face attacks causing negative effect by causing battery exhaustion and higher energy utilization.

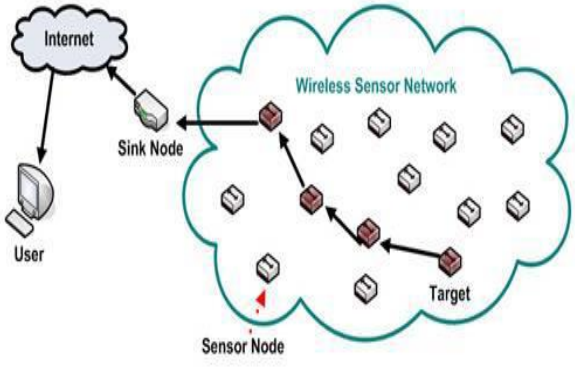


Fig 1: Ad hoc Wireless sensor network

Vampire attacks are caused when a message is been initiated and transmitted through a malicious node over the network causing higher battery utilization and battery exhaustion. Vampire attacks are not constrained to a specific type of protocol and does not alter specific path in the network. When a network is been attacked by them, even transfer of small data consumes more energy.

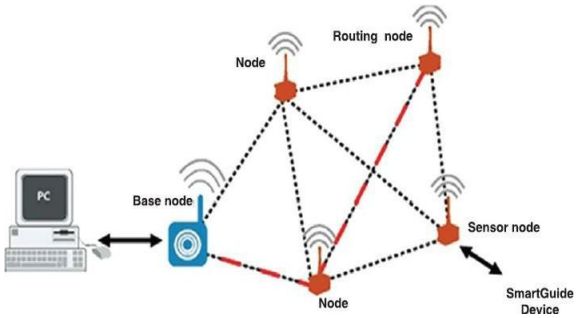


Fig 2: Architecture of WSN

The basic architecture of a WSN [10] contains number of nodes that act as routing nodes, sensing nodes and base nodes. Figure 2 shows the architecture of a WSN, where all the different types of nodes are shown. It is also possible that every node in the network functions as an aggregation point, delaying transmission of an outgoing message until a sufficient number of incoming messages have been received and aggregated. Power management in sensor networks is critical. Consequently, if we want sensor networks to last for years, it is crucial that they run at around a 1% duty cycle (or less). Similarly, since the power consumption of the radio is three orders of magnitude higher when transmitting or listening than when in sleep mode, it is crucial to keep the radio in sleep mode the overwhelming majority of the time.

Sensor networks provide economically viable solutions for a wide variety of applications, including surveillance of critical infrastructure, safety monitoring, and many health-care applications [6]. As sensor networks are increasingly deployed in such security-and safety critical environments, the need for secure communication primitives is self-

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

evident. Likewise, the development of such primitives facilitates the use of sensor networks in a wider range of applications. The central goal of this work is to ensure node-to-node message delivery, even if the sensor network is under active attack [8]. The presence of an attacker, it is an extremely challenging task to maintain correct routing information; the attacker could inject malicious routing information or alter routing setup/update messages from legitimate nodes. Even when route setup/update messages are authenticated, compromised sensor nodes can supply incorrect routing information of their own and cripple the routing infrastructure.

WSNs consist of nodes they are independent and have no infrastructure. The nodes of WSN consists of Data acquisition unit, Data transfer unit and Process unit to which power is supplied as shown in the figure 3. These nodes are used in different fields to gather information in different ways. Base stations are typically many orders of magnitude more powerful than sensor nodes [12]. They might have workstation or laptop class processors, memory, and storage, AC power, and high bandwidth links for communication amongst themselves.

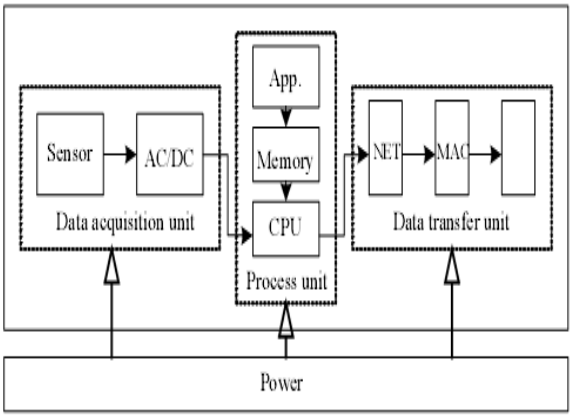


Fig 3: Nodes of WSN

The sensors are constrained to use lower-power, lower-bandwidth, shorter-range radios, and so it is envisioned that the sensor nodes would form a multi-hop wireless network to allow sensors to communicate to the nearest base station. A base station might request a steady stream of data, such as a sensor reading every second, from nodes able to satisfy a query [9]. We refer to such a stream as a data flow and to the nodes sending the data as sources.
In order to reduce the total number of messages sent and thus save energy, sensor readings from multiple nodes may be processed at one of many possible aggregation points.

An aggregation point collects sensor readings from surrounding nodes and forwards a single message representing an aggregate of the values. Aggregation points [3] are typically regular sensor nodes, and their selection is not necessarily static. Aggregation points could be chosen dynamically for each query or event.

II. PROTOCOLS AND ASSUMPTIONS

In this paper we discuss the effect of vampire attacks on Ad-hoc On Demand Vector Routing (AODV) [5]. AODV is a reactive protocol for ad-hoc and a mobile network that maintains routes only between nodes which need to communicate. The routing messages do not contain information about the entire route path, but only about the source and destination. Therefore routing messages don't not have an increasing size. It uses destination sequence numbers to specify how fresh a route is, which is used to grant loop freedom. As seen in figure 4, whenever a node needs to send a packet to a destination for which it has no „fresh enough" route (i.e., a valid route entry for the destination whose associated sequence number is at least as great as the ones contained in any RREQ that the node has received for that destination) it broadcasts a route request (RREQ) message to its neighbors. Each node that receives the broadcast sets up a reverse route towards the originator of the RREQ (unless it has a „fresher" one). When the intended destination (or an intermediate node that has a „fresh enough" route to the destination) receives the RREQ, it replies by sending a Route Reply (RREP). It is important to note that the only mutable information in a RREQ and in a RREP is the hop count (which is being monotonically increased at each hop). The RREP travels back to the originator of the RREQ (this time as a unicast). At each intermediate node, a route to the destination is set (again, unless the node has a „fresher" route than the one specified in the RREP). In the case that the RREQ is replied to by an intermediate node (and if the RREQ had set this option), the intermediate node also sends a RREP to the destination. In this way, it can be granted that the route path is being set up bidirectional. In the case that a node receives a new route (by a RREQ or by a RREP) and the node already has a route „as fresh" as the received one, the shortest one will be updated.

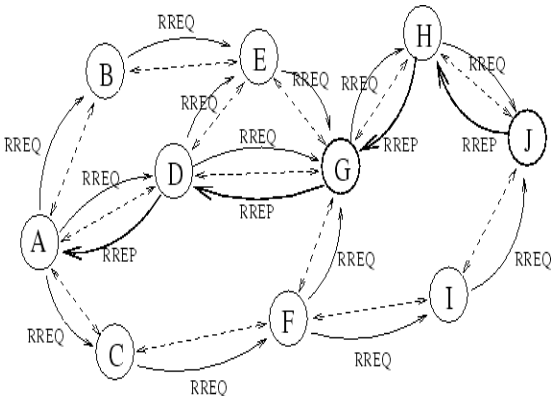


Fig 4: AODV protocol

If there is a subnet (a collection of nodes that are identified by a common network prefix) that does not use AODV as its routing protocol and wants to be able to exchange information with an AODV network, one of the nodes of the subnet can be selected as their „network leader". The network leader is the only node of the subnet that sends forwards and processes AODV routing messages and

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

every RREP that the leader issues, it sets the prefix size of the subnet optionally. A Route Reply Acknowledgment (RREP-ACK) message may be sent by the originator of the RREQ to acknowledge the receipt of the RREP. RREP-ACK message has no mutable information. In addition to these routing messages, Route Error (RERR) message are used to notify the other nodes that certain nodes are not anymore reachable due to a link breakage.

When a node rebroadcasts a RERR, it only adds the unreachable destinations to which the node might forward messages. Therefore, the mutable information in a RERR is the list of unreachable destinations and the counter of unreachable destinations included in the message. Anyway, it is predictable that, at each hop, the unreachable destination list may not change or become a subset of the original one. The vampire attack disrupts the AODV protocols ability to avoid loops and choose the shortest path, AODV are prone to wormhole attacks [14] and false injection of data [7] which can be avoided by using an encryption system [7] [13] [11].

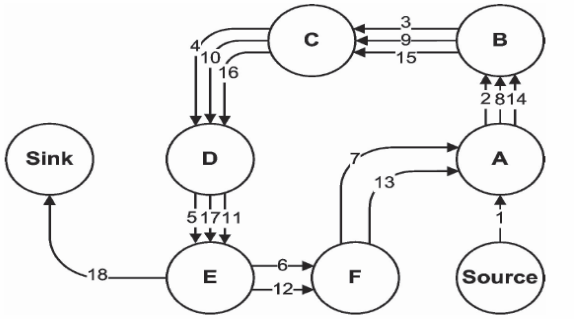
III. VAMPIRE ATTACK DETECTION

There are two types of attacks in WSN, the routing depletion and resource depletion attack. The routing depletion attacks usually only affect the routing path the resource depletion attacks are the ones that attack the network features like bandwidth, power, and energy consumption. These attacks are commonly called as "Vampire attacks" [2]. They are called so because they drain the battery power from the nodes. These are a type of Denial of Service [1] since they affect the entire system from performing. They are difficult to be detected since they are protocol compliant and are orthogonal to them [4]. They are not protocol specific.

They do not affect a single node they take their time attack one by one and disrupt the entire system. Vampire attacks can be defined as the composition and transmission of a message that cause more energy to be consumed by the network than if an honest node transmitted a message of identical size to the same destination, although using different packet headers. The strength of the attack is measured by the ratio of network energy used in the benign case to the energy used in the malicious case. Safety from Vampire attacks implies that this ratio is 1. Energy use by malicious nodes is not considered, since they can always unilaterally drain their own batteries.

A. Carousel attack

In this attack, an adversary composes packets with purposely introduced routing loops. It is called carousel attack, since it sends packets in circles as shown in Figure 4. It 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. On average, a random located carousel attacker in the example mentioned topology can increase the network energy consumption by a factor of 1.48±0.99.



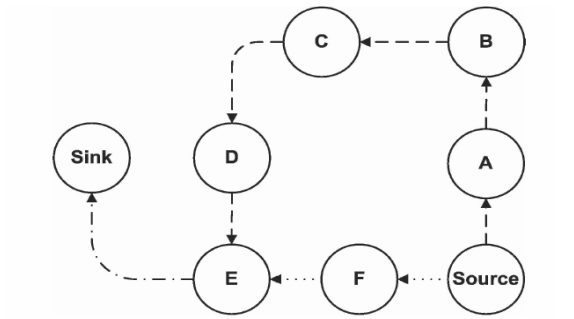
(a) An honest route would exit the loop immediately from node E to Sink, but a malicious packet makes its way around the loop twice more before exiting.

Fig 5: Carousel attack

The reason for this large standard deviation is that the attack does not always increase energy usage, the length of the adversarial path is a multiple of the honest path, which is in turn, affected by the position of the adversary's position of the adversary in relation to the destination, so the adversary's position is important to the success of this attack. Figure 5 shows the network under attack where the packets are sent in loops causing more usage of energy and time.

B. Stretch attack

In this attack, also targeting source routing, an adversary constructs artificially long routes, potentially traversing every node in the network. It is call this the stretch attack, since it 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. An example is illustrated in figure 6. In the example topology, there is an increase in energy usage by as much as a factor of 10.5 per message over the honest scenario, with an average increases in energy consumption of 2.67±2.49. As with the carousel attack, the reason for the large standard deviation is that the position of the adversarial node affects the strength of the attack. Not all routes can be significantly lengthened, depending on the location of the adversary.



(b) Honest route is dotted while malicious route is dashed. The last link to the sink is shared.

Fig 6: Stretch attack

The carousel attack, where the relative positions of the source and sink are important, the stretch attack can achieve the same effectiveness independent of the attacker's network position relative to the destination, so

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

the worst-case effect is far more likely to occur .The impact of these attacks can be further increased by combining them, increasing the number of adversarial nodes in the network, or simply sending more packets. Although in networks that do not employ authentication or only use end-to-end authentication, adversaries are free to replace routes in any overhead packets, we assume that only messages originated by adversaries may have maliciously composed routes.

IV. SECURITY AGAINST VAMPIRE ATTACKS

A Clean Slate Sensor Network Routing by PLGP (Parno, Luk, Gaustad and Perrig) can be applied which consists of two phases:
I. Topology Discovery Phase
II. Packet Forwarding Phase

I. Topology Discovery Phase:
A node starts with its virtual address as zero. At each node a certificate is been issues which contains the public key for identification. Each node is connected to the other and shares virtual address, public key and the certificate when they merge with closest nearby group.

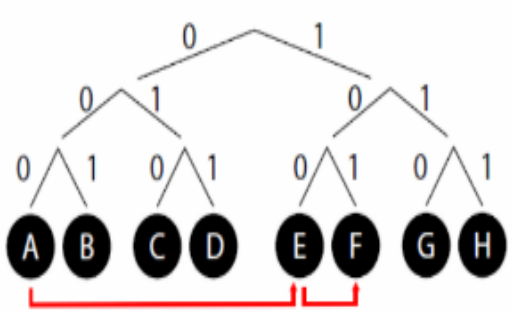


Fig 7: Topology Discovery Phase

II. Packet Forwarding Phase:
The packets are forwarded in this phase as shown in figure 8.

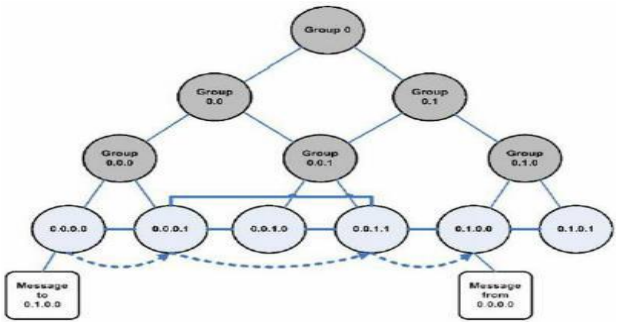


Fig 8: Packet Forwarding Phase

PLGP proposed a solution which suggests:
a. Providing a verifiable path history to all the packets involved.
b. Using this path history the packet transmission can take place through every node securely passing through at least one honest node.
c. Each node upon receiving the message, checks for authentication in the chain.

CONCLUSION

In this paper, the routing protocol affected by vampire attack in WSN is discussed. This is a new class of resource consumption attack that use routing protocols to permanently disable ad-hoc WSNs by depleting node's battery power. Simulation results show that depending on the location of adversary, network energy expenditure during the forwarding phase increasing. The security flaws of AODV can be fixed by using RSA encryption system that will avoid the adversary from entering the system. These attacks does not depend on particular type of protocol and Ad hoc network sensors have been applied in various fields which needs to create and identify solutions for prevention of the network from these attacks. There are different types of vampire attacks depending on the protocol. When the attack take place it not only consumes higher power but also takes additional time. There are many solutions and techniques that have been presented to prevent these attacks but were not effective enough which creates a need for a better solution. PLGP solutions can be applied to these protocols in order to prevent these networks that are often prone to vampire attacks.

REFERENCES

[1]. A. Wood and J. Stankovic. Denial of Service in sensor networks. IEEE Computer, pages 54-62, Oct, 2002.
[2]. Eugene Y. Vassermann and Nicholas Hopper "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks" IEEE Trans. Mobile Computing, vol. 12, no. 2, pp. 318-332 Feb-2013.
[3]. .B. Przydatek, D. Song, and A. Perrig. SIA:Secure information aggregation in sensor network. In ACM SenSys, Nov 2003.
[4]. B. Karp and H. T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks." In mobile Computing and Networking, 2000, pp.243-254.
[5]. C. Perkins and E. Royer, "Ad-hoc on demand distance vector routing," in MILCOM ˝97 panel on Ad Hoc Networks, 1997.
[6]. Chris Karloff and David Wager "Secure Routing in Wireless Sensor Networks: Attacks and countermeasures" Proc. IEEE Int˝l workshop sensor network protocols and applications, 2003.
[7]. F. Ye, H. Luo and S. "Statistical En-Route Filtering of Injected False Data in Sensor Networks," IEEE Journal on Selected Areas in Communication, vol. 23, No.4, 2005, pp.839-8.
[8]. H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.
[9]. J. Deng, R. Han, and S. Mishra, "Maximum Lifetime Routing in Wireless Sensor Networks," IEEE/ACM Trans. Networking, vol 12. 4, pp. 609-619, Aug. 2004.
[10]. J.Hill, R.Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, "System architecture directions for networked sensors," in Proceedings of ACM ASPLOS IX, November 2000.
[11]. L. Buttyan, et al., "Statistical Wormhole Detection in Sensor Networks," Lecture Notes in Computer Science Vol. 3813, 2005, pp. 128-141.
[12]. M. Tubaishat and S. Madria, "Sensor Networks: An Overview," IEEE Potentials, Vol. 22, No. 2, 2003, pp. 20-23. doi:10.1109/MP.2003.1197877.
[13]. M. McLoone and M. Robshaw, "Public Key Cryptography and RFID Tags," Proc. RSA conf. Cryptography, 2006.
[14] Y.C, Hu, A.Perrig, and D.B. Johnson, "Wormhole detection in wireless ad hoc networks," Department of Computer Science, Rice University, Tech. Rep TR01-384, June 2002.