Vampire Attacks in Wireless Ad-Hoc Sensor Network for Sheltering Data Packets

[1]Rajesh Khanna.M, [2]Dr.A.Rengarajan, [3]A.Aravindan
[1]Research Scholar, Department of Computer science and Engineering, St.Peter's University, Avadi, Chennai, India.
[2]Professor, Department of Computer science and Engineering, Veltech Multitech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi, Chennai, India.
[3]PG scholar, Department of Information Technology, Veltech Multitech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi, Chennai, India.

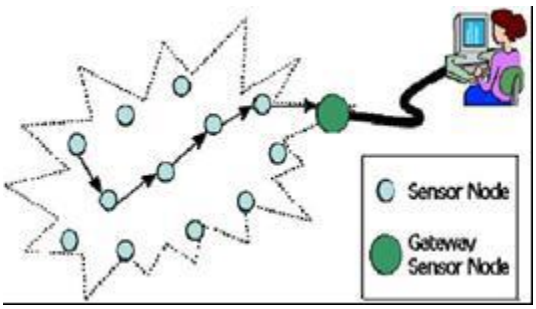
***Abstract* — In sensing and common computing ad hoc low-power wireless networks are an exciting research direction. Earlier security scheme in this area has focused mainly on denial of communication at the routing or medium access control levels. This paper redefines resource depletion attacks at the routing protocol layer. This attack permanently disables networks by quickly draining nodes' battery power. These "Vampire" attacks are not specific to any specific protocol, but depend on the properties of many popular classes of routing protocols. We discussed all protocols are susceptible to Vampire attacks, which are dangerous, difficult to detect, and are very easy to carry out using very few such as one malicious insider sending only protocol-compliant messages. With this, a single Vampire can increase network-wide energy usage by a factor of O(N), here N in the number of network nodes in the network. Proposed algorithm finds the solution for carousal attack and stretch attack to achieve better security. Also trust based energy efficient technique is adopted to keep network active in vampire attack, it also help to detect and avoid malicious nodes in the routing phase**

Key words—Denial of service, security, routing, ad-hoc networks, Sensor networks, wireless network.

I. INTRODUCTION

Ad hoc wireless sensor networks introduces exciting schemes in the future, such as all consumed on-demand computing power, continuous connectivity, quick deployable communication for military and first responders. These kinds of networks already monitor environmental conditions, factory performance, and malicious nodes' group deployment, to name a few applications. Now a days WSNs become more critical to the everyday functioning of people and organizations, also availability faults become less tolerable— unavailability can make the difference between business and lost productivity, power outcome, environmental crises, and lost lives; so high availability of these networks is an important property, and should hold even under critical conditions. Because of their ad hoc organization wireless ad hoc networks are specifically resistant to denial of service (DoS) attacks.

A wireless sensor network (WSN) of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications. . 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.



While these schemes can prevent attacks on the short-term availability of a network, they do not address attacks that affect long-term availability—the most permanent denial of service attack is to entirely deplete nodes' batteries. This is an instance of a resource depletion attack, with battery power as the resource of interest. In this paper, we consider how routing protocols, even those designed to be secure, lack protection from these attacks, which we call Vampire attacks, since they drain the life from networks nodes.

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. Neither do these attacks rely on flooding the network with large amounts of data, but rather try to transmit as little data as possible to achieve the largest energy drain,

preventing a rate limiting solution. Since Vampires use protocol-compliant messages, these attacks are very difficult to detect and prevent.

We define a Vampire attack as the composition and transmission of a message that causes 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. We measure the strength of the attack by the ratio of network energy used in the benign case to the energy used in the malicious case, i.e., the ratio of network-wide power utilization with malicious nodes present to energy usage with only honest nodes when the number and size of packets sent remains constant.

A. Protocols And Assumptions

The routing protocols such as link-state, distance-vector, source routing and geographic and beacon routing protocols, as well as a logical ID-based sensor network routing protocol proposed by Parno et al. all can be affected by Vampire attacks.

All routing protocols employ at least one topology discovery period, since ad hoc deployment implies no prior position knowledge. Limiting ourselves to immutable but dynamically organized topologies, as in most wireless sensor networks, we further differentiate 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. Our adversaries are malicious insiders and have the same resources and level of network access as honest nodes. Furthermore, adversary location within the network is assumed to be fixed and random, as if an adversary corrupts a number of honest nodes before the network was deployed, and cannot control their final positions. Note that this is far from the strongest adversary model; rather this configuration represents the average expected damage from Vampire attacks. Intelligent adversary placement or dynamic node compromise would make attacks far more damaging.

While for the rest of this paper we will assume that a node is permanently disabled once its battery power is exhausted, let us briefly consider nodes that recharge their batteries in the field, using either continuous charging or switching between active and recharge cycles. In the continuous charging case, power-draining attacks would be effective only if the adversary is able to consume power at least as fast as nodes can recharge.

Assuming 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. However, recall that sending any packet automatically constitutes amplification, allowing few Vampires to attack many honest nodes. We will show later that a single Vampire may attack every network node simultaneously, meaning that continuous recharging does not help unless Vampires are more resource constrained than honest nodes. Dual-cycle networks (with mandatory sleep and awake periods) are equally vulnerable to Vampires during active duty as long as the Vampire's cycle switching is in sync with other nodes. Vampire attacks may be weakened by using groups of nodes with staggered cycles: only active-duty nodes are vulnerable while the Vampire is active; nodes are safe while the Vampire sleeps. However, this defence is only effective when duty cycle groups outnumber Vampires, since it only takes one Vampire per group to carry out the attack.

B. Overview

In the remainder of this paper, we present a series of increasingly damaging Vampire attacks, evaluate the vulnerability of several example protocols, and suggest how to improve resilience. In source routing protocols, we show how a malicious packet source can specify paths through the network which are far longer than optimal, wasting energy at intermediate nodes that forward the packet based on the included source route. In routing schemes, where forwarding decisions are made independently by each node (as opposed to specified by the source), we suggest how directional antenna and worm-hole attacks [30] 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.

In our first attack, an adversary composes packets with purposely introduced routing loops. We call it the carousel attack, since it sends packets in circles as shown in Fig. 1a. 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. Brief mentions of this attack can be found in other literature [10], but neither intuition for defence nor any evaluation is provided. In our second attack, also targeting source routing, an adversary constructs artificially long routes, potentially traversing every node in the network. We 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 Fig. 1b.

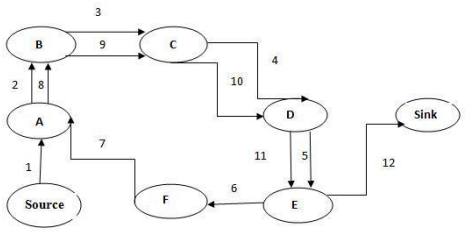


Fig. 1a) True route would exit the loop immediately from node E to sink, but an attack packet makes its way around the loop twice more before exiting.

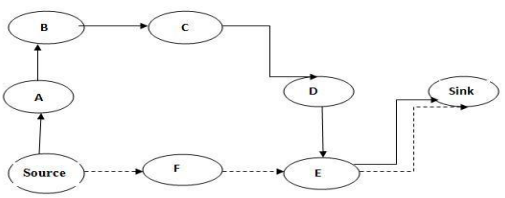


Fig. 1b) True route is dotted while attacked route is dashed

II. RELATED WORK

In this section, we will see the some of the related works to the intrusion detection of vampire in the wireless ad hoc networks using different approaches. A very early mention of power exhaustion can be found in, as "sleep deprivation torture." As per the name, the proposed attack prevents nodes from vampire attack.

Here shows that destination sequence distant vector a proactive network routing protocol can be modified to provably resist Vampire attacks during the packet forwarding phase. Even though the existing DSDV is designed to overcome routing loop problems, it is still not a feasible method for efficient packet transmission, as the protocol is proactive which utilizes more battery power and bandwidth. M-DSDV consists of a topology discovery phase, followed by a topology maintenance phase [1]. The source address and destination address are the internet protocol addresses, the sequence number is used to differentiate new routes from stale routes, the next hop and metric is a local counter maintained separately by each node and incremented each time a RReq is broadcasted, the index number is initialized to zero, is used to keep track of the loops the packet has made and the final time to live field is used as a clock which increments whenever a RReq packet is sent.

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 [2]. 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 protocolcompliant messages.

Entering a low-power sleep cycle, and thus depletes their batteries faster. Newer research on "denial-of-sleep" only considers attacks at the MAC layer Additional work mentions resource exhaustion at the MAC and transport layer but only offers rate limiting and elimination of insider adversaries as potential solutions. Malicious cycles (routing loops) have been briefly mentioned [10] but no effective defences are discussed other than increasing efficiency of the underlying MAC and routing protocols or switching away from source routing.

There is also significant past literature on attacks and defences against quality of service (QoS) degradation, or RoQ attacks, that produce long-term degradation in net-work performance [23], [26]. The focus of this work is on the transport layer rather than routing protocols, so these defences are not applicable. Moreover, since Vampires do not drop packets, the quality of the malicious path itself may remain high (although with increased latency).

Other work on denial of service in ad hoc wireless networks has primarily dealt with adversaries who prevent route setup, disrupt communication, or preferentially establish routes through themselves to drop, manipulate, or monitor packets [14], [28], [29]. The effect of denial or degradation of service on battery life and other finite node resources has not generally been a security consideration, making our work tangential to the research mentioned above. Protocols that define security in terms of path discovery success, ensuring that only valid network paths are found, cannot protect against Vampire attacks, since Vampires do not use or return illegal routes or prevent communication in the short term.

Current work in minimal-energy routing, which aims to increase the lifetime of power-constrained networks by using less energy to transmit and receive packets (e.g., by minimizing wireless transmission distance) [11], [15], [19] is likewise orthogonal: these protocols focus on cooperative nodes and not malicious scenarios

Additional on power-conserving MAC, upper layer protocols, and cross-layer cooperation [24] However, Vampires will increase energy usage even in minimal-energy routing scenarios and when power-conserving MAC protocols are used; these attacks cannot be prevented at the MAC layer or through cross-layer feedback. Attackers will produce packets which traverse more hops than necessary, so even if nodes spend the minimum required energy to transmit packets, each packet is still more expensive to transmit in the presence of Vampires. Our work can be thought of attack-resistant minimal-energy routing, where the adversary's goal includes decreasing energy savings.

Deng et al. discuss path-based DoS attacks and defences in [13], including using one-way hash chains to limit the number of packets sent by a given node, limiting the rate at which nodes can transmit packets. While this strategy may protect against traditional DoS, where the malefactor overwhelms honest nodes with large amounts of data, it does not protect against "intelligent" adversaries who use a small number of packets or do not originate packets at all. As an example of the latter, Aad et al. show how protocol-compliant malicious intermediaries using intelligent packet-dropping strategies can significantly degrade performance of TCP streams traversing those nodes. Our adversaries are also protocol compliant in the sense that they use well-formed routing protocol messages. However, they either produce messages when honest nodes would not, or send packets with protocol headers different from what an honest node would produce in the same situation.

III. PROPOSED WORK

In this section, we show that a clean-slate secure sensor network routing protocol by Parno et al. ("PLGP" from here on) 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.

In PLGP, forwarding nodes do not know what path a packet took, allowing adversaries to divert packets to any part of the network, even if that area is logically further away from the destination than the malicious node. This makes PLGP vulnerable to Vampire attacks. Consider for instance the now-familiar directional antenna attack: a receiving honest node may be farther away from the packet destination than the malicious forwarding node, but the honest node has no way to tell that the packet it just

received is moving away from the destination; the only information available to the honest node is its own address and the packet destination address, but not the address of the previous hop (who can lie). Thus, the Vampire can move a packet away from its destination without being detected.

A. Security Against Vampire Attacks:

Here, we modify the forwarding phase of PLGP to provably avoid the above-mentioned attacks. First we introduce 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

B. Detection And Mitigation Of Vampire Attacks

As the paper has now clearly illustrated the way in which Vampire attacks develop in a network and its devastating effects on the network. We are now in position to now design a mechanism or technique by which we can minimize this effect such attack. In a WSN network when packet of message is sent from source node (sender) to sink node (receiver), it is forwarded by intermediate nodes present in the network and this carries flow continues till it reaches the sink node. In the proposed system we overcome the Vampire attack by performing various validation that ensures that packets doesn't go into infinite loop causing drainage of battery and crashing of network. For validation we define function Secure_packet_forward (p).

Secure_packet_forward (p)

1) S← extract _source_add (p);
2) a← extract_attestation (p);
3) c←closest_ next_ hop (s);
4) for each node that sends packet
5) if attestation (a) verification fails
6) Drop packet (p)
7) Else // if matches
8) Retrieves next hop info to the requested node in the selected shortest path
9) Return the c← closest next hop IP/Port number to requesting node
10) Forward packet (p) to node (c)

The resulting protocol, PLGP with attestations (PLGPa) uses this packet history 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 node n forwards packet p, it this by attaching a nonreplayable 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.

C. PLGPa Concept In IDS

This PLGPa concept we use it in IDS: An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports.

In the above algorithm when IDS receives any request packet from any node it calculates the shortest path between the sender and destination and it checks i)the attestation of packet ie source and destination address and signature chain and ii) is the node logically closer to the destination than the previous node in the chain.

This way IDS can enforce the forward progress a of packet, then IDS transmits the next closest hop IP address and port number in the shortest path to the requested node if the attestation were valid otherwise it discards the packet at the node itself to mitigate the vampire attacks.

IV. AODV NETWORK ROUTING

In this section, we show that Ad hoc On-Demand Distance Vector a reactive network routing protocol. AODV network routing is a routing protocol for mobile ad hoc networks (MANETs) and other wireless ad hoc networks. It can be modified to provably resist vampire attacks during the packet forwarding phase. Even though the existing DSDV is designed to overcome routing loop problems, it is still not a feasible method for efficient packet transmission, as the protocol is proactive which utilizes more battery power and bandwidth. AODV consists of routes established On-demand connection is low. Thus, when a link fails, a routing error is passed back to a transmitting node and process repeats. When a source node S, wants to send a data packet to destination D, first constructs and broadcasts a route request packet consisting of (source address, destination address, sequence number, next hop, metric, index number and time to live) fields. The source address and destination address are the internet protocol addresses, the sequence number is used to differentiate new routes from stale routes, the next hop and metric is a local counter maintained separately by each node and incremented each time a RReq is broadcasted, the index number is initialized to zero, is used to keep track ofthe loops the packet has made and the final time to live field is used as a clock which increments whenever a RReq packet is sent. AODV works only when a data is delivered from source node S, wants to send data packet to destination D. It maintains the route to destination D.

V. CONCLUSION

Our proposed technique in this paper, address the properties of routing protocol attacks in the wireless ad hoc networks In order to overcome the vampire or malicious attacks in WSN, the information transmission is carried in the trusted path of the networks. Our proposed technique addresses the vampire attacks in the wireless ad hoc networks when compared to the existing approaches. In the vampire attack, the two types of attacks may arisen the entire networks into collapse, total energy consumption level increases, and allocates long routing path and so on. And the two types of attacks are: In the Carousel attack, attackers introduce some packet within a route tranquil as a sequence of loops, such that the same node appears in the route of communication many times and the other attack is stretch attack also targeting resource steering, attackers construct falsely long routes, potentially traversing every node in the network. And also stretch attack, increases packet lane length, causing packets to be processed by a number of nodes that is self-governing of hop count down the straight path stuck between the challenger and packet

target. This attack increases the routing length and delay very much in the networks and also inadequate by the number of allowable entries in the resource route. In this paper we also proposed new technique to detect the misbehaviour nodes in the wireless ad hoc networks. Our experimental result showed that our proposed novel technique works efficiently when compared to previous methods.

REFERENCES

1. Rajesh Khanna M, S.Divya, Dr. A. Rengarajan. "Securing Data Packets from Vampire Attacks in Wireless Ad-Hoc Sensor Network", International Journal of Innovative Research in Computer and communication Engineering(IJIRCC), Vol.2 Year March,2104.
2. Eugene Y. Vasserman and Nicholas Hopper. Vampire attacks: Draining life from wireless ad-hoc sensor networks, IEEE Transactions on Mobile Computing Vol.12 No.2 Year 2013
3. G. Acs, L. Buttyan, and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 5, no. 11, pp. 1533-1546, Nov. 2006.
4. T. Aura, "Dos-Resistant Authentication with Client Puzzles," Proc. Int'l Workshop Security Protocols, 2001.
5. J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," Proc. 12th Conf. USENIX Security, 2003.
6. D. Bernstein and P. Schwabe, "New AES Software Speed Records," Proc. Ninth Int'l Conf. Cryptology in India: Progress in Cryptology (INDOCRYPT), 2008.
7. D.J. Bernstein, "Syn Cookies," http://cr.yp.to/syncookies.html, 1996.
8. I.F. Blaked, G. Seroussi, and N.P. Smart, Elliptic Curves in Cryptography, vol. 265. Cambridge Univ., 1999.
9. J.W. Bos, D.A. Osvik, and D. Stefan, "Fast Implementations of AES on Various Platforms," Cryptology ePrint Archive, Report 2009/ 501, http://eprint.iacr.org, 2009.
10. H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.
11. J.-H. Chang and L. Tassiulas, "Maximum Lifetime Routing in Wireless Sensor Networks," IEEE/ACM Trans. Networking, vol. 12, no. 4, pp. 609-619, Aug. 2004.
12. T.H. Clausen and P. Jacquet Optimized Link State Routing Protocol (OLSR), IETF RFC 3626, 2003.
13. J. Deng, R. Han, and S. Mishra, "Defending against Path-Based DoS Attacks in Wireless Sensor Networks," Proc. ACM Workshop Security of Ad Hoc and Sensor Networks, 2005.
14. J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-Tolerant Routing for Wireless Sensor Networks," Computer Comm., vol. 29, no. 2, pp. 216-230, 2006.
15. S. Doshi, S. Bhandare, and T.X. Brown, "An On-Demand Minimum Energy Routing Protocol for a Wireless Ad Hoc Network," ACM SIGMOBILE Mobile Computing and Comm. Rev., vol. 6, no. 3, pp. 50-66, 2002.
16. J.R. Douceur, "The Sybil Attack," Proc. Int'l Workshop Peer-to-Peer Systems, 2002.
17. H. Eberle, A. Wander, N. Gura, C.-S. Sheueling, and V. Gupta, "Architectural Extensions for Elliptic Curve Cryptography over GF(2m) on 8-bit Microprocessors," Proc. IEEE Int'l Conf' Applica-tion-Specific Systems, Architecture Processors (ASAP), 2005.
18. T. English, M. Keller, K.L. Man, E. Popovici, M. Schellekens, and W. Marnane, "A Low-Power Pairing-Based Cryptographic Accel-erator for Embedded Security Applications," Proc. IEEE Int'l SOC Conf. , 2009.
19. L.M. Feeney, "An Energy Consumption Model for Performance Analysis of Routing Protocols for Mobile Ad Hoc Networks," Mobile Networks and Applications, vol. 6, no. 3, pp. 239-249, 2001.
20. M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong Authentication for RFID Systems Using the AES Algorithm," Proc. Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES), 2004.
21. R. Fonseca, S. Ratnasamy, J. Zhao, C.T. Ee, D. Culler, S. Shenker, and I. Stoica, "Beacon Vector Routing: Scalable Point-to-Point Routing in Wireless Sensornets," Proc. Second Conf. Symp. Networked Systems Design & Implementation (NSDI), 2005.
22. S. Galbraith, K. Harrison, and D. Soldera, "Implementing the Tate Pairing," Proc. Int'l Symp. Algorithmic Number Theory, 2002.
23. S. Goldberg, D. Xiao, E. Tromer, B. Barak, and J. Rexford, "Path-Quality Monitoring in the Presence of Adversaries," Proc. ACM SIGMETRICS Int'l Conf. Measurement and Modeling of Computer Systems, 2008.