Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.1083 – 1091

RESEARCH ARTICLE

THE EFFECT OF VAMPIRE ATTACKS ON DISTANCE VECTOR ROUTING PROTOCOLS FOR WIRELESS AD HOC SENSOR NETWORKS

Jagadeesh[1], Joseph William[2]

[1]PG Scholar, Department of Electrical and Electronics Engineering, Sri Muthukumaran Institute of Technology Chennai, India

[2]Assistant Professor, Department of Electrical and Electronics Engineering, Sri Muthukumaran Institute of Technology Chennai, India

jagadeesh.jagan2@gmail.com [1], williamkdcfs@gmail.com [2]

Abstract-- The aim of this project is to define Vampire attacks, a new class of resource consumption attacks that use distance vector routing protocols to permanently disable ad hoc wireless sensor networks by depleting nodes' battery power. 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. Dual-cycle networks 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 defense is only effective when duty cycle groups out number Vampires, since it only takes one Vampire per group to carry out the attack.

Keywords-- Denial of service, security, routing, ad hoc networks, sensor networks, wireless networks

I. INTRODUCTION

The fast paced progress in the Ad Hoc Wireless Sensor Networks (WSNs) has enabled the use of a number of wireless applications on the move. 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.

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.

The negligence of study in this area has provided the grounds for research of the same. The main objective of this project is to investigate the available Vampire attack mitigation methods and compare the performances in different protocols and to demonstrate the same through suitable simulation results.

The first challenge in addressing Vampire attacks is defining them—what actions in fact constitute an attack? DoS attacks in wired networks are frequently characterized by amplification [25]: an adversary can amplify the resources it spends on the attack, e.g., use 1 minute of its own CPU time to cause the victim to use 10 minutes. However, consider the process of routing a packet in any multihop network: a source composes and transmits it to the next hop toward the destination, which transmits it further, until the destination is reached; consuming resources not only at the source node but also at every node the message moves through. If we consider the cumulative energy of an entire network, amplification attacks are always possible, given that an adversary can compose and send messages which are processed by each node along the message path. So, the act of sending a message is in itself an act of amplification, leading to resource exhaustion, as long as the aggregate cost of routing a message (at the intermediate nodes) is lower than the cost to the source to compose and transmit it. So, we must drop amplification as our definition of maliciousness and instead focus on the cumulative energy consumption increase that a malicious node can cause while sending the same number of messages as an honest node.

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. 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.

II. RELATED WORK

We do not imply that power draining itself is novel, but rather that these attacks have not been rigorously defined, evaluated, or mitigated at the routing layer. A very early mention of power exhaustion can be found in [21], as "sleep deprivation torture." As per the name, the proposed attack prevents nodes from 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 [29]. Additional work mentions resource exhaustion at the MAC and transport layers [45], [34] but only offers rate limiting and elimination of insider adversaries as potential solutions. Malicious cycles (routing loops) have been briefly mentioned [10], [35], but no effective defenses are discussed other than increasing efficiency of the underlying MAC and routing protocols or switching away from source routing.

Even in non-power-constrained systems, depletion of resources such as memory, CPU time, and bandwidth may easily cause problems. A popular example is the SYN flood attack, wherein adversaries make multiple connection requests to a server, which will allocate resources for each connection request, eventually running out of resources, while the adversary, who allocates minimal resources, remains operational (since he does not intend to ever complete the connection handshake). Such attacks can be defeated or attenuated by putting greater burden on the connecting entity (e.g., SYN cookies [7], which offload the initial connection state onto the client, or cryptographic puzzles [4], [45], [37]). These solutions place minimal load on legitimate clients who only initiate a small number of connections, but deter malicious entities who will attempt a large number. Note that this is actually a form of rate limiting, and not always desirable as it punishes nodes who produce burst traffic but may not send much total data over the lifetime of the network. Since Vampire attacks rely on amplification, such solutions may not be sufficiently effective to justify the excess load on legitimate nodes.

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 network performance [23], [26], [41], [42], [44], [17], [29]. The focus of this work is on the transport layer rather than routing protocols, so these defenses 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], [36], .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], [36] 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], [34], [43], [45]. 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 [2]. 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. Another attack that can be thought of as path based is the wormhole attack, first introduced in [30]. It allows two non-neighbouring malicious nodes with either a physical or virtual private connection to emulate a neighbour relationship, even in secure routing systems [3]. These links are not made visible to other network members, but can be used by the colluding nodes to privately exchange messages. Similar tricks can be played using directional antennas. These attacks deny service by disrupting route discovery, returning routes that traverse the wormhole, and may have artificially low associated cost metrics (such as number of hops or discovery time, as in rushing attacks [31]). While the authors propose a defence against wormhole and directional antenna attacks (called "Packet Leashes" [30]), their solution comes at a high cost and is not always applicable. First, one flavor of Packet Leashes relies on tightly synchronized clocks, which are not used in most of the self-devices.

III. SYSTEM ANALYSIS

A. Existing system

Wireless ad hoc networks are particularly vulnerable to denial of service (DoS) attacks. Prior security work in this area has focused primarily on denial of communication at the routing or medium access control levels. These attacks are distinct from previously studied DoS, 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 attacks.

B. Proposed system

In the proposed systems 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 defense is only effective when duty cycle groups outnumber Vampires, since it only takes one Vampire per group to carry out the attack.

Also we present a series of increasingly damaging Vampire attacks, evaluate the vulnerability of several example protocols, and suggest how to improve resilience.

IV. ATTACKS ON STATELESS PROTOCOLS

Here, we present simple but previously neglected attacks on source routing protocols, such as DSR [35]. In these systems, the source node specifies the entire route to a destination within the packet header, so intermediaries do not make independent forwarding decisions, relying rather on a route specified by the source. To forward a message, the intermediate node finds itself in the route (specified in the packet header) and transmits the message to the next hop. The burden is on the source to ensure that the route is valid at the time of sending, and that every node in the route is a physical neighbour of the previous route hop. This approach has the advantage of requiring very little forwarding logic at intermediate nodes, and allows for entire routes to be sender authenticated using digital signatures, as in Ariadne [29].

We evaluated both the carousel and stretch attacks in a randomly generated 30-node topology and a single randomly selected malicious DSR agent, using the ns- 2 network simulator [1]. Energy usage is measured for the minimum number of packets required to deliver a single message, so sending more messages increases the strength of the attack linearly until bandwidth saturation. We independently computed resource utilization of honest and malicious nodes and found that malicious nodes did not use a disproportionate amount of energy in carrying out the attack. In other words, malicious nodes are not driving down the cumulative energy of the network purely by their own use of energy. Nevertheless, malicious node energy consumption data are omitted for clarity. The attacks are carried out by a randomly selected adversary using the least intelligent attack strategy to obtain average expected damage estimates. More intelligent adversaries using more information about the network would be able to increase the strength of their attack by selecting destinations designed to maximize energy usage.

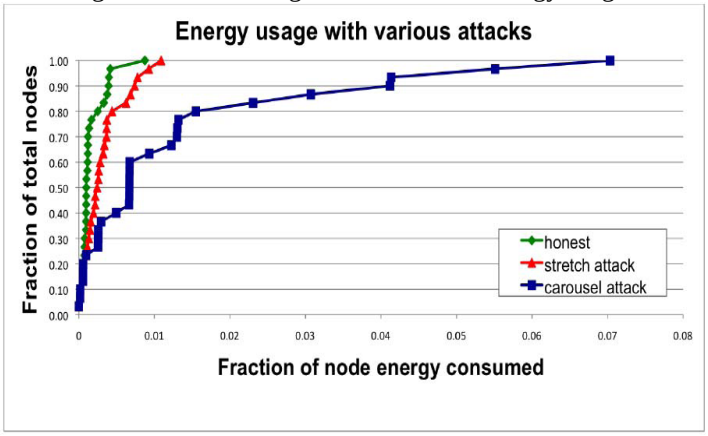


Fig. 1. Node energy distribution under various attack scenarios. The network is composed of 30 nodes and a single randomly positioned Vampire. Results shown are based on a single packet sent by the attacker.

Per-node energy usage under both attacks is shown in Fig. 2. As expected, the carousel attack causes excessive energy usage for a few nodes, since only nodes along a shorter path are affected. In contrast, the stretch attack shows more uniform energy consumption for all nodes in the network, since it lengthens the route, causing more nodes to process the packet. While both attacks significantly network-wide energy usage, individual nodes are also noticeably affected, with some losing almost 10 percent of their total energy reserve per message. Fig. 3a diagrams the energy usage when node 0 sends a single packet to node 19 in an example network topology with only honest nodes.
Black arrows denote the path of the packet.

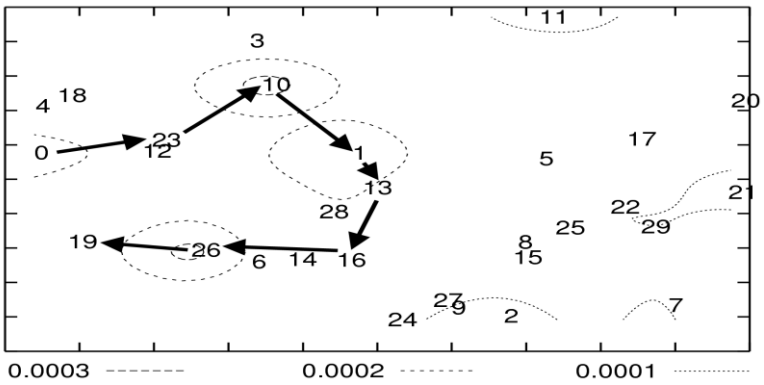


Fig.2.Honest scenario: node 0 sends a message to node19

A. Carousel attack

In this attack, an adversary sends a packet with a route composed as a series of loops, such that the same node appears in the route many times. This strategy can be used to increase the route length beyond the number of nodes in the network, only limited by the number of allowed entries in the source

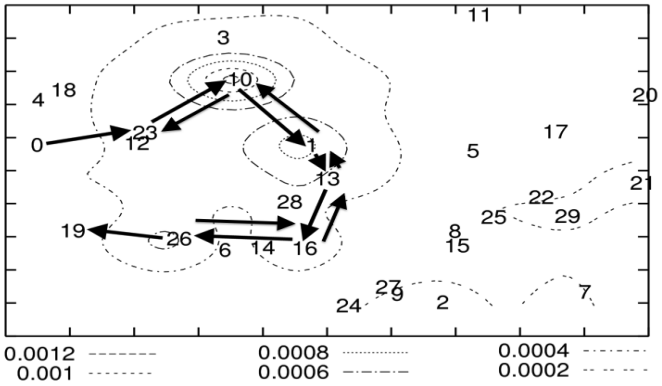
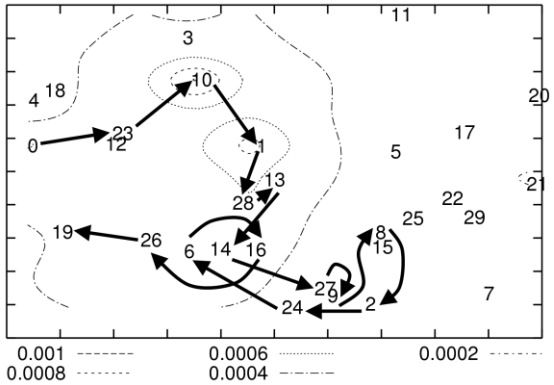


Fig. 3 Carousel attack(malicious node 0)

In Fig. 3, malicious node 0 carries out a carousel attack, sending a single message to node 19 (which does not have to be malicious). Note the drastic increase in energy usage along the original path.3 Assuming the adversary limits the transmission rate to avoid saturating the network, the theoretical limit of this attack is an energy usage increase factor of O(λ), where λ is the maximum route length.

Overall energy consumption increases by up to a factor of 3.96 per message. On average, a randomly located carousel attacker in our example topology can increase network energy consumption by a factor of 1:48 _ 0:99. 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 in relation to the destination.

B. Stretch attack.



Another attack in the same vein is the 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-> F ->E ->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.

Fig 4.Stretch attack (malicious node 0)

The outcome becomes clearer when we examine Fig. 3c and compare to the carousel attack. While the latter uses energy at the nodes who were already in the honest path, the former extends the consumed energy "equivalence lines" to a wider section of the network. Energy usage is less localized around the original path, but more total energy is consumed. The theoretical limit of the stretch attack is a packet that traverses every network node, causing an energy usage increase of factor O(min(N, λ))where N is the

number of nodes in the network and λ is the maximum path length allowed. This attack is potentially less damaging per packet than the carousel attack, as the number of hops per packet is bounded by the number of network nodes. However, adversaries can combine carousel and stretch attacks to keep the packet in the network longer: the resulting "stretched cycle" could be traversed repeatedly in a loop. Therefore, even if stretch attack protection is not used, route loops should still be detected and removed to prevent the combined attack. In our example topology, we see an increase in energy usage by as much as a factor of 10.5 per message over the honest scenario, with an average increase 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. Unlike 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 the worst case effect is far more likely to occur.

V. Mitigation Methods

The carousel 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 malicious environments. The ns-2 DSR protocol does implement loop detection, but confusingly does not use it to check routes in forwarded packets.5 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 [29]. Therefore, it is better to simply drop the packet, especially considering that the sending node is likely malicious (honest nodes should not introduce loops). An alternate solution is to alter how intermediate nodes process the source route.

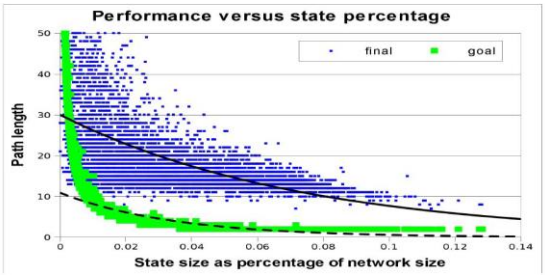


Fig. 5. Loose source routing performance compared to optimal, in a network with diameter slightly above 10. The dashed trend line represents expected path length when nodes store logN local state, and the solid trend line shows actual observed performance

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 (the last instance of the local node will be found in the source route rather than the first). No extra processing is required for this defence; since a node must perform this check anyway we only alter the way the check is done.

The stretch attack is more challenging to prevent. Its success rests on the forwarding node not checking for optimality of the route. If we call the no-optimization case "strict" source routing, since the route is followed exactly as specified in the header, we can define loose source routing, where intermediate nodes may replace part or all of the route in the packet header if they know of a better route to the destination. This makes it necessary for nodes to discover and cache optimal routes to at least some fraction of other nodes, partially defeating the as-needed discovery advantage. Moreover, caching must be done carefully lest a maliciously suboptimal route be introduced.

We simulated the loose source routing defence using random-length suboptimal paths in randomly generated network topologies of up to 1,000,000 nodes, with diameter 10-14. Results (Fig. 5) demonstrate that the amount of node-local storage required to achieve reasonable levels of mitigation approaches global topology knowledge, defeating the purpose of using source routing. The dashed trend line represents the expected path length of rerouted packets if each node stores log N network paths, where N is the number of network nodes, while the solid trend line represents the majority of actual network paths in a loose source-routing setup.

The number of nodes traversed by loose source routed packets is suboptimal by at least a factor of 10, with some routes approaching a factor of 50. Only a few messages encountered a node with a better path to the destination than the originally assigned long source route. Therefore we conclude that loose source routing is worse than keeping global state at every node. Alternatively, we can bound the damage of carousel and stretch attackers by limiting the allowed source route length based on the expected maximum

path length in the network, but we would need a way to determine the network diameter.6 While there are suitable algorithms [40],there has been very little work on whether they could yield accurate results in the presence of adversaries.

If the number of nodes is known ahead of time, graph-theoretic techniques can be used to estimate the diameter. Rate limiting may initially seem to be a good defence, but upon closer examination we see it is not ideal. It limits malicious sending rate, potentially increasing network lifetime, but that increase becomes the maximum expected lifetime, since adversaries will transmit at the maximum allowed rate. Moreover, sending rate is already limited by the size of nodes' receive queues in rate-unlimited networks Rate limiting also potentially punishes honest nodes that may transmit large amounts of time-critical (bursty) data, but will send little data over the network lifetime.

VI. PERFORMANCE ANALYSIS

The performance of the proposed scheme is evaluated by means of the network simulator. The simulation results bring out some important characteristic functions of the proposed methods. In this section we record the various parameters of the simulation by using record procedure. The recorded events are stored in the trace files. By executing the trace files by using x graph or gnu plot we can get the graph as the output. The energy usage in the attack model can be assessed and compared with the energy usage after the application of mitigation methods in the network.

The bandwidth overhead of our attestation scheme is minimal, as chain signatures are compact (less than 30 bytes). Comparatively, a minimum-size DSR route request packet with no route, payload, or additional options is 12 bytes [35]; we used 512-byte data packets in our simulations. The additional and width, therefore, is not significant, increasing per-packet transmit power by about 4:8 _J, plus roughly half for additional power required to receive. Energy expenditure for cryptographic operations at intermediate hops is, unfortunately, much greater than transmit or receive overhead, and much more dependent on the specific chipset used to construct the sensor. However, we can make an educated guess about expected performance and power costs. Highly optimized software only implementations of AES-128, a common symmetric cryptographic primitive, require about 10 to 15 cycles per byte of data on modern 32-bit x86 processors without AE Specific instruction sets or cryptographic co-processors [6].

Due to the rapid growth in the mobile space and increased awareness of security requirements, there has been significant recent work in evaluating symmetric and asymmetric cryptographic performance on inexpensive and low-power devices. report AES-128 performance on 8-bit microcontrollers of 124.6 and 181.3 CPU cycles per byte [9], and Feldhofer et al. Report just over 1,000 cycles per byte using low-power custom circuits[20]. Surprisingly, although asymmetric cryptography is generally up to two orders of magnitude slower than symmetric, McLoone and Robshaw demonstrate a fast and low-power implementation of an asymmetric cryptosystem
for use in RFID tags [42].

VII. CONCLUSION

In this paper, 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-concepts 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. Simulation results show that depending on the location of the adversary, network energy expenditure during the forwarding phase increases from between 50 to 1,000 per cent By using the mitigation methods, the attacks in the wireless sensor networks are greatly reduced. The power consumption by the nodes due to the vampire attacks is greatly reduced and resilience to the network was provided. The performance analysis by using the X-graph also shows the improvement of the system behavior under different attacks.

REFERENCES

[1] I. Aad, J.-P. Hubaux, and E.W. Knightly, "Denial of Service Resilience in Ad Hoc Networks," Proc. ACM MobiCom,2012.
[2] A.J. Goldsmith and S.B. Wicker, "Design Challenges for Energy- Constrained Ad Hoc Wireless Networks," IEEE Wireless Comm., vol. 9, no. 4, pp. 8-27, Aug. 2012
[3] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," Computer, vol. 36, no. 10, pp. 103-105, Oct. 2010.

[4] 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. 2013.
[5] L. Xiaojun, N.B. Shroff, and R. Srikant, "A Tutorial on Cross-Layer Optimization in Wireless Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 8, pp. 1452-1463, Aug. 2012.
[6]Volkan Rodoplu and Teresa H. Meng" Minimum Energy Mobile Wireless Networks" IEEE journal on selected areas in communications, vol. 17, no. 8, august 2011
[7] Ivan Stojmenovic and Xu Lin "Power-Aware Localized Routing in Wireless Networks" IEEE transactions on parallel and distributed systems, vol. 12, no. 11, November 2011
[8] Jun Yuan, Zongpeng Li, Wei Yu and Baochun Li "A Cross-Layer Optimization Framework for Multihop Multicast in Wireless Mesh Networks" IEEE journal on selected areas in communications, vol. 24, no. 11, November 2006
[9] David R. Raymond and Scott F. Midkiff "Denial-of-Service in Wireless Sensor Networks: Attacks and Defences" Published by the IEEE CS 2010 IEEE
[10] 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, vol. 58, no. 1, January 2009
[11] Gergely A´ cs, Levente Buttya´n, and Istva´n Vajda "Provably Secure On-demand Source Routing in Mobile Ad Hoc Networks" IEEE journal March 2010
[12] Jason L. Hill, David E. Culler "MICA: A WIRELESS PLATFORM FOR DEEPLY EMBEDDED NETWORKS" IEEE Transaction 2012
[13] Ray-Guang Cheng, Shin-Ming Cheng, and Phone Lin, "Power-Efficient Routing Mechanism for ODMA Systems" IEEE transactions on vehicular technology, vol. 55, no. 4, July 2006
[14] Chia-Mu Yu,Yao-Tung Tsou, Chun-Shien Lu, and Sy-Yen Kuo "Constrained Function-Based Message Authentication for Sensor Networks" IEEE transactions on information forensics and security, vol. 6, no. 2, June 2011
[15] Jing Deng, Richard Han, and Shivakant Mishra "Defending against Path based DoS Attacks in Wireless Sensor Networks" 2009 4th IEEE International Conference.
[16] Tuomas Aura, Pekka Nikander and Jussipekka Leiwo "DOS-resistant Authentication with Client Puzzles" IEEE conference August 2010 Networks" 6t Annual ACM/IEEE International Conference on Mobile Computing and
[17] Brad Karp and H. T. Kung "GPSR: Greedy Perimeter Stateless Routing for Wireless Networking (MobiCom 2010).
[18] J. Deng, R. Han, and S. Mishra "INSENS: Intrusion-tolerant routing for wireless sensor networks," Computer Communications, (2006), vol. 29(2), pp. 216-230.
[19] R. L. Rivest, A. Shamir, and L. Adleman "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" February 2011 vol. 21. No. 2 COMMUNICATION OF THE ACM
[20] Vasudevan .A. "Risks and Security of Internet and Systems (CRISIS)", 2009 Fourth International Conference
[21]Mangai.S,.Tamilarasi,A.;Venkatesh,C."Dynamic core multicast routing protocol implementation using ANT colony optimization in ad hoc wireless networks Computing", Communication and Networking, 2008.
[22]Slijepcevic.S,Potkonjak.M.,Tiatsis.,Zimbeck, S. ; Srivastava, M.B. "On communication security in wireless ad-hoc sensor networks" Enabling Technologies: Infrastructure for Collaborative Enterprises, 2012.
[23]Ngai,E.C.-H.,Lyu, M.R. "An authentication service based on trust and clustering in wireless ad hoc networks: description and security evaluation" 2006. IEEE International Conference on
[24] Safdar, G.A. ,McGrath, C., McLoone, M "Existing Wireless Network Security Mechanisms and their Limitations for Ad Hoc Networks" Irish and simulation of dynamic and rapid auto-configuration protocols for ad-hoc wireless
[25] Vaidyanathan, R. ,Kant, L. ; McAuley, A. ; Bereschinsky, M. "Performance modeling Networks" Simulation Symposium, 2010. 36th Annual
[26] M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang, "Reduction of Quality (RoQ) Attacks on Internet End-Systems," Proc. IEEE INFOCOM, 2005.
[27] J.L. Hill and D.E. Culler, "Mica: A Wireless Platform for Deeply Embedded Networks," IEEE Micro, vol. 22, no. 6, pp. 12-24, Nov./ Dec. 2002.
[28] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Proc. IEEE Workshop Mobile Computing Systems and Applications, 2002.
[29] Y.-C. Hu, D.B. Johnson, and A. Perrig, "Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks," Proc. MobiCom, 2002.

[30] Y.-C. Hu, D.B. Johnson, and A. Perrig, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks," Proc. IEEE INFOCOM, 2003.
[31] Y.-C. Hu, D.B. Johnson, and A. Perrig, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," Proc.Second ACM Workshop Wireless Security (WiSE), 2003.
[32] Y. Huang and S. Bhatti, "Fast-Converging Distance Vector Routing for Wireless Mesh Networks," Proc. 28th Int'l Conf. Distributed Computing Systems Workshops (ICDCSW), 2008.
[33] D. Hwang, B.-C. Lai, P. Schaumont, K. Sakiyama, Y. Fan, S. Yang, A. Hodjat, and I. Verbauwhede, "Design Flow for HW/SW Acceleration Transparency in the Thumbpod Secure Embedded System," Proc. Design Automation Conf., 2003.
[34] L. Iannone, R. Khalili, K. Salamatian, and S. Fdida, "Cross-Layer Routing in Wireless Mesh Networks," Proc. Int'l Symp. Wireless Comm. Systems, 2004.
[35] D.B. Johnson, D.A. Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks," Ad Hoc Networking, Addison-Wesley, 2001.
[36] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. IEEE Int'l Workshop Sensor Network Protocols and Applications, 2003.
[37] B. Karp and H.T. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks," Proc. ACM MobiCom, 2000.
[38] Y. Kawahara, T. Takagi, and E. Okamoto, "Efficient Implementation of Tate Pairing on a Mobile Phone Using Java," Proc. Int'l Conf. Computational Intelligence and Security, 2006.
[39] M. Koschuch, J. Lechner, A. Weitzer, J. Groschdl, A. Szekely, S. Tillich, and J. Wolkerstorfer, "Hardware/Software Co-Design of
Elliptic Curve Cryptography on an 8051 Microcontroller," Proc. Eighth Int'l Conf. Cryptographic Hardware and Embedded Systems
(CHES), 2006.
[40] A. Kro¨ ller, S.P. Fekete, D. Pfisterer, and S. Fischer, "Deterministic Boundary Recognition and Topology Extraction for Large Sensor Networks," Proc. Ann. ACM-SIAM Symp. Discrete Algorithms, 2006.
[41] A. Kuzmanovic and E.W. Knightly, "Low-Rate TCP-Targeted Denial of Service Attacks: The Shrew vs. the Mice and Elephants" Proc. SIGCOMM, 2003.
[42] Y.-K. Kwok, R. Tripathi, Y. Chen, and K. Hwang, "HAWK:Halting Anomalies with Weighted Choking to Rescue Well- Behaved TCP Sessions from Shrew DDoS Attacks," Proc. Int'l Conf. Networking and Mobile Computing, 2005.
[43] L. Xiaojun, N.B. Shroff, and R. Srikant, "A Tutorial on Cross-Layer Optimization in Wireless Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 8, pp. 1452-1463, Aug. 2006.
[44] X. Luo and R.K.C. Chang, "On a New Class of Pulsing Denial-of- Service Attacks and the Defense," Proc. Network and Distributed System Security Symp. (NDSS), 2005.
[45] M. Maleki, K. Dantu, and M. Pedram, "Power-Aware Source Routing Protocol for Mobile Ad Hoc Networks," Proc. Int'l Symp. Low Power Electronics and Design (ISLPED), 2002.

ABOUT THE AUTHORS

Mr. S.JAGADEESH is currently a student of Sri Muthukumaran Institute of technology, Chennai and he is doing his Masters in "Embedded System Technology". He received his Bachelors degree in Electrical and Electronics Engineering from Bethlahem Institute of Engineering, Kanyakumari on 2012.His area of interest includes Wireless Sensor Networks and in Embedded Systems.

Mr. Joseph William is an assistant professor in Department of Electrical and Electronics Engineering, Sri Muthukumaran Institute of technology, Chennai. He received his Master degree in Applied Electronics from Sri Muthukumaran Institute of technology, Chennai, on 2012.He received his Bachelors degree in Electrical and Electronics Engineering from D.M.I. College of Engineering, Chennai on 2008.His area of work involves in Wireless Sensor networks

