www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242

Volume 3 Issue 5, May 2014, Page No. 5801-5806

Protection from Vampire Attacks on Routing Protocol

Pushpalata D. Chandore[1], Devendra Vatsa[2], Nitesh Rastogi[3]

[1] PG Student at JDCT

[2]Assistant Professor at JDCT

[3]HOD at JDCT Indore, MP, India

nishtha.pushpalata@gmail.com dev.vatsa11@gmail.com rastogi.nitesh@gmail.com

***Abstract*-In sensing and pervasive computing ad-hoc low-power wireless networks are an exciting research. Prior security work has first focused on denial of communication at the routing or levels of media access control. This paper examine resource depletion attacks at routing protocol layer, which disable networks by quickly draining node's battery power. These "Vampire" attacks are not specific to any particular protocol, but rather depend on the properties of many well known classes of routing protocols. We find that all examined protocols are affected to Vampire attacks ,which are destructing, hard to detect, and are easy to carry out using as few as one malicious insider sending only protocol compliant messages. In case of worst case, a single Vampire can increase network-wide energy usage by a factor of O(N), where N in the number of nodes of network. The methods we discuss to mitigate these types of attacks which includes a new proof-of- concept protocol that bounds the damage caused by Vampires during the packet forwarding phase.**

INDEX TERMS

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

I. INTRODUCTION

In future ad-hoc wireless sensor networks (WSNs) will present exciting new applications, such as on-demand computing power, continuous connectivity and instantly-deployable communication for first responders and military. These networks already consider environmental conditions, factory performance, and troop deployment, to name some applications. Now-a-days WSN become more popular but its functioning towards the people and industry is bulky so the reasons behind it -lack of availability of network, lost productivity, power outages, environmental distruction, and even lost lives. So to overcome these we can use the wireless ad-hoc network. These methods can stop attacks from happening on the short-term availability of a network but they do not address attacks that affect long-term availability — the most permanent denial of service attack is to completely distruct battery life of node. This system also consider how routing protocols lack security from vampire attacks since they drain the life from nodes in the networks. These attacks are different from previously-seen DoS, reduction of quality (RoQ), and routing infrastructure attacks as they do not disrupt immediate availability, but work over time to completely disable a network. Vampire attacks are not protocol-specific and they do not depend on design properties or implementation faults of specific routing protocols, but rather exploit properties of protocol classes such as link-state, distance-vector, source routing, and geographic and beacon routing. Vampire attacks do not depend on flooding the network with large amounts of data rather try to transmit as little data as possible to get the largest energy drain which prevents a rate limiting solution. These attacks are very hard to detect and prevent because Vampires use protocol-compliant messages.

Evaluate the vulnerabilities of existing protocols to routing layer battery reduction attacks. Existing work on secure routing attempts to confirm that intruder cannot cause path discovery to return an invalid network path, but Vampires do not modify discovered paths instead of that it uses existing valid network paths and protocol compliant messages. Protocols that increases power efficiency are also inappropriate because they depend on cooperative node behaviour and cannot optimize out malicious work. To bound the damage from Vampire attacks during forwarding of packets modify an existing sensor network routing protocol .The effect of Vampire attacks are consider on link-state, distance vector, source routing and beacon routing protocols also a logical ID-based sensor network routing protocol. According to above stated protocols we view the covered protocols as an important subset of the routing solution that our attacks are likely to apply to other protocols. All routing protocols employ at least one topology discovery period. Our attackers are malicious insiders having the same resources and level of network access as honest nodes. Attacker location within the network is assumed to be fixed and random. This is far from the strongest adversary model; rather this configuration represents the average expected damage from Vampire attacks. Smart adversary placement or dynamic node compromise would make attacks far more damaging. While for the rest of the project will assume that a node is permanently disabled once its battery power is exhausted, consider nodes that recharge their batteries in the place, using either continuous charging or switching between active and recharge cycles. In case of continuous charging , power-draining attacks would be effective only if the adversary is able to consume power at least as fast as nodes can recharge. Considering 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.

II. LITERATURE SURVEY

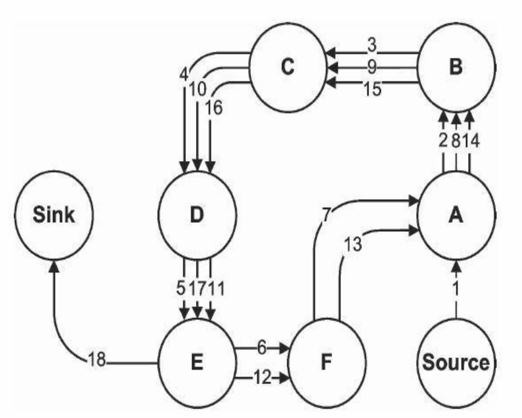
We do not imply that power draining itself is novel, but these attacks have not been defined, evaluated, or mitigated at the routing layer. Power exhaustion can be found in [13], as “sleep deprivation torture.” The attack prevents nodes from entering a low-power sleep cycle, and deplete their batteries faster. The new research on “denial of-sleep” only considers attacks at the medium access control(MAC) layer [11]. It also mentions resource exhaustion at the MAC and transport layers [12, 15], but offers rate limiting and elimination of insider attackers as potential solutions. Malicious cycles (routing loops) are briefly mentioned [2, 10], but no effective defences are discussed other than increasing efficiency of the MAC and routing protocols away from source routing. In non-power-constrained systems, reduction of resources such as memory, CPU time, and bandwidth may easily cause problems. A well-known example is the SYN flood attack, where attackers make multiple connection requests to a server, which in turn will allocate resources for each connection request, eventually running out of resources, while the attacker, who allocates less resources, remains operational(since he does not intend to complete the connection handshake). These attacks can be defeated by putting greater load on the connecting entity. These solutions place less load on legitimate clients who only initiate a small number of connections, but deter malicious entities who will attempt a large number. This is actually a form of rate limiting, and not always desirable as it punishes nodes who create bursty traffic but does not send much total data over the lifetime of the network. Since Vampire attacks depend on amplification, such solutions does not be sufficiently effective to justify the large load on legitimate nodes. There is a past literature on attacks and defences against quality of service (QoS) degradation, or reduction of quality (RoQ) attacks, that create long-term reduction in network performance [6, 7]. The main focus of this work is on the transport layer rather than routing protocols, so these defences are not applicable. Since Vampires do not drop packets, the quality of the malicious path remain high. Other work on denial of service in ad-hoc wireless networks has primarily deal with attackers who prevent route setup, disrupt communication, or establish routes through themselves to drop, manipulate, or monitor packets. The effect of denial of service on the life of battery and other finite node resources has not been a security consideration, making our work tangential to the research mentioned above. Protocols which specify security in terms of path discover y success, ensuring that only valid network paths are found, cannot protect against Vampire attacks because Vampires do not use or return illegal routes or prevent communication in the short term. The current work in minimal-energy routing, which increases the lifetime of power-constrained networks by using less energy to transmit and receive packets[3,5] is orthogonal: these protocols focus on cooperative nodes and not malicious scenarios. In minimal-energy routing scenarios Vampires will increase energy usage and these attacks cannot be prevented at the MAC layer or through cross-layer feedback when power-conserving MAC protocols are used. Attackers will create packets which traverse more hops than require, so even if nodes consume less required energy to transmit packets, each packet is still more costly to transmit in the presence of Vampires. Our work can be thought of attack-resistant minimal-energy routing, where the attacker’s goal includes decreasing savings in energy. The scientist Deng et al. discuss path based DoS attacks and defences in [4], 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. This strategy protects against traditional DoS, where the malefactor overwhelms honest nodes with large amounts of data, it does not protect against “intelligent” attackers who use a small number of packets or do not originate packets at all. Using intelligent packet-dropping strategies, the scientist Aad et al. show how protocol-compliant malicious intermediaries can significantly degrade performance of TCP streams traversing those nodes [1]. Our attackers are also protocol-compliant in the sense that they use well-formed routing protocol messages. However, they either create messages when honest nodes would not, or send packets with protocol headers distinct from what an honest node would produce in the same situation. Another path-based attack is the wormhole attack, first introduced in [9]. With either a physical or virtual private connection it allows two non-neighbouring malicious nodes to emulate a neighbour relationship, even in secure routing systems. These links are not made visible to other members of network, 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 have artificially low associated cost metrics. The authors propose a defence against wormhole and directional antenna attacks but their solution comes at a high cost which is not always applicable. The authors assume that packet travel time dominates processing time, which is not be borne out in latest wireless networks, particularly low power wireless sensor networks.

III. METHODOLOGY

A. *Attack on Stateless Protocols*

Attacks that targets source routing are mention below

(a) Carousel attack: attacker creates packets with purposely introduced routing loops and sends packets in circles that targets source routing protocols by exploiting the limited verification of message headers at forwarding nodes that allows a single packet to repeatedly travel through the same set of nodes. In carousel attack, an attacker sends a packet with a route which consists of a series of loops, such that the same node appears in the route more than one time. This strategy can be used to increase the length of the route beyond the number of nodes in the network which is only limited by the number of allowed entries in the source route.



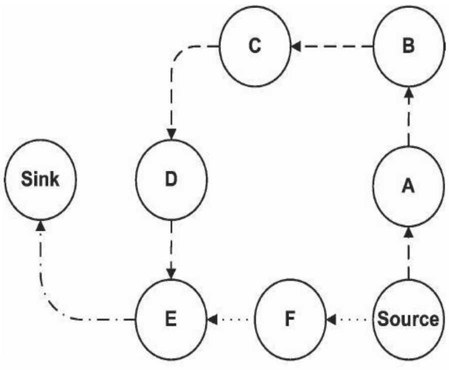
(a) An honest route would exit the loop immediately from node E to Sink, but a malicious packet makes its way around the loop twice more before exiting.

1) Algorithm for Carousel Attack

```
Carousel_Attack(ip_address,packet)
{
Extract the source address
Find next closest neighbour.
If(next!=receiver)
{
Forward the packet.
ip=neighbour_ip.
Carousel_Attack(ip_address,packet)
}
}
```

(b)Stretch attack

In stretch attack, where a malicious node constructs artificially long source routes which causes 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. An attacker creates long routes, traversing ever y node in the network and also increases packet path lengths, causing packets to be processed by a number of nodes.



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

2) Algorithm for Stretch Attack

```
Stretch_Attack(ip_address)
{
Extract the closest neighbour
If(neighbour!=listed)
{
if (neighbour!=receiver)
{
Forward packet.
}
Stretch_Attack(ip_addres,packet)
}
}
```

3) Algorithm for Carousel Attack Prevention

```
Carousel_Attack(ip_address,packet)
{
Extract closest neighbour
if(closest_neighbour!=listed)
{
Forward packet(ip_address,packet)
}
}
```

4) Prevention of Stretch Attack

Source will first find send primary key using RSA algorithm to the receiver and also then source will send message in encrypted form. After receiving a message from source , receiver will match key with the message and after it gets verified the message will get decrypted.

B. *Attack on Stateful Protocols*

1. Directional antenna attack

When forwarding decisions are made independently by each node then vampires have small control over packet progress but they can still waste energy by restarting a packet in various parts of the network. Using a directional antenna attackers can insert a packet in any parts of the network,also while forwarding the packet locally. It uses the energy of nodes that would have to process the original packet, with the expected honest energy expenditure of O(d), where d is the diameter of network. This attack can be said as a half-wormhole attack [9], as directional antenna constitutes a private communication channel. It can be performed more than once by inserting the packet at various distant points in the network, at the additional cost to the attacker for each use of the directional antenna. Packet Leashes cannot stop from happening this attack because they are not made to protect against malicious message sources, only intermediaries [9].

2. Malicious discovery attack

In most of the protocols, every node will forward route discovery packets , that means it is possible to initiate a flood by sending a single message. Systems AODV and DSR perform as-needed route discovery are vulnerable, since nodes may initiate discover y at any time, not just during change in a topology. A malicious node has a number of ways to activate topology change: it may wrongly claim that claim a new link or a link is down to a non existent node. Two cooperating malicious nodes may claim that the link between them is down but nearby nodes may able to monitor communication to detect failure of link. But still failures in less distance route can be ignored in networks of sufficient density. When nodes claim that a long distance route are changed , more serious attacks may possible. In open networks with unauthenticated routes, this attack is trivial because a single node can emulate multiple nodes in neighbour relationships, or wrongly claim nodes as neighbours. Hence, assume closed networks where link states are authenticated, just like route authentication in Ariadne [8] or path-vector signatures in [14]. To execute the attack attacker must present an actually changed route. For that purpose, two cooperating attackers that communicates through a wormhole must repeatedly announce and withdraw routes that use this wormhole, which causes a theoretical energy usage increase of a factor of O(N) per packet. The number of possible route announce or withdrawal pairs increases by adding more malicious nodes to the mix. Packet Leashes [9] cannot prevent this attack because the originators themselves are malicious, they could forward messages through the wormhole, and return only valid routes in response to discover y. This problem is similar to route flapping in BGP, but while Internet paths are stable paths change frequently in wireless ad-hoc networks, where nodes moves in and out of each other's range. This solution could not be applicable because there may be no stable routes in WSNs.

A. Coordinate and beacon-based protocols

Coordinate and beacon-based routing are GPSR and BVR, which uses physical coordinates or beacon distances for routing respectively. In GPSR, a packet encounters a dead end, which is a localized space of minimal physical distance to the sink, but without the sink actually being reachable. Then the packet must be diverted until a path to the sink is available. Packets are routed in BVR toward the beacon closest to the sink node, and then move away from the beacon to reach the sink. Each node makes independent forwarding decisions and thus a Vampire is limited in the distance it can divert the packet.

IV. CLEAN-SLATE SENSOR NETWORK ROUTING(PLGP)

It is developed by the scientist Parno,Luk, Gaustad and Perrig (PLGP).Its original version is vulnerable to vampire attacks and can be modified to prevent vampire attacks. It consist of two phases:

1. Topology Discovery Phase
2. Packet Forwarding phase

Topology discovery organizes nodes to trees. Initially each node knows only itself and at end of discover y each node should compute the same address tree as other nodes. All leaf nodes are physical nodes in network and virtual addresses corresponds to their position in the network.

Topology discovery Phase

In this phase, every node broadcast certificate of identity including public key. Each node starts as its own group size one ,having virtual address zero. Groups are merge with smallest neighbouring group and each group chooses 0 or 1 when merge with another group. Each member prepends group address to their own address gateway nodes. At the end each node knows every nodes virtual address ,public key and certificate and then network converges to a single group.

Packet forwarding Phase

In this phase, all decisions are made independently by each node. When a node receives a packet determines next hop by finding the most significant bit of its address that varies from the message originators address. Every forwarding event shortens the logical distance to destination.

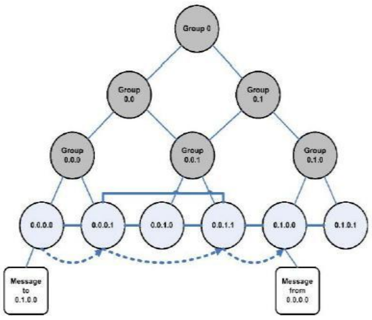


Fig. 6. The final address tree for a fully converged six-node network. Leaves represent physical nodes, connected with solid lines if within radio range. The dashed line is the progress of a message through the network. Note that nonleaf nodes *are not physical nodes* but rather logical group identifiers.

B. PLGP in presence of Vampires

Forwarding nodes don't know the path of a packet and allows attackers to divert packet to any part of the network. Honest node may be far away from the destination than malicious nodes but honest node knows only its address and the address of destination. Vampire moves packet away from the destination. Theoretical energy increase of O(d) where d is the network diameter and N the number of network nodes. In the worst case packet returns to vampire as it can reroute.

V. PROVABLE SECURITY AGAINST VAMPIRE ATTACKS

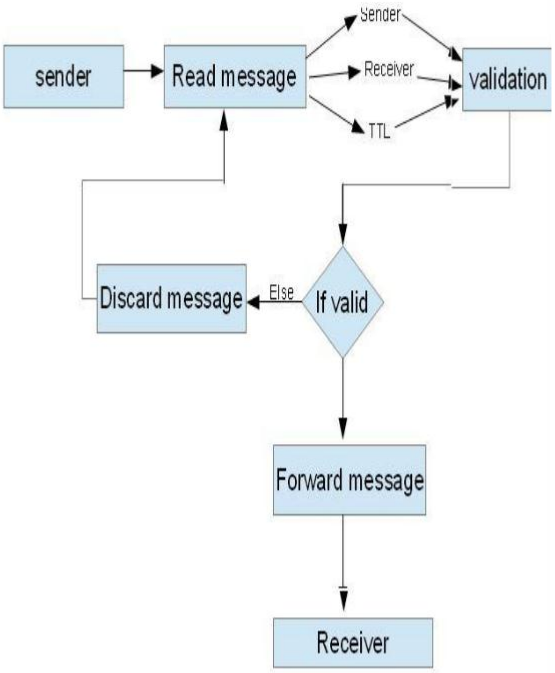
No-backtracking property: Satisfied for a given packet if and only if it consistently makes progress toward its destination in the logical network address space. More formally: No-backtracking is satisfied if ever y packet p traverses the same number of hops whether or not an adversary is present in the network. Nodes keep track of route cost.Nobacktracking implies Vampire resistance.PLGP does not satisfy No-backtracking property: In PLGP packets are forwarded along the shortest route through the tree that is allowed by the physical topology. The tree implicitly reflects the topology and every node keeps a similar copy of the address tree, every node can check the optimal next logical hop. This is not sufficient for no-backtracking to hold because nodes cannot be certain of the path previously traversed by a packet. Adversaries can always lie about their local metric cost. PLGP is still vulnerable.

VI. PROPOSED SYSTEM

A. Propose PLGP with attestations (PLGPa):

Add a verifiable path history to every PLGP packet**.**PLGPa uses this packet history together with PLGP's tree routing structure so every node can securely verify progress which prevents any significant adversarial influence on the path taken by any packet which traverses at least one honest node. These signatures form a chain attached to every packet and allows any node receiving it to validate its path. To ensure that the packet has never travelled away from its destination in the logical address space, every forwarding node verifies the attestation chain.

PLGPa satisfies no-backtracking- All messages are signed by their originator. Attacker can only alter packet fields that are changed enroute, so only the route attestation field can be altered, shortened, or removed entirely. Use one-way signature chain construction to prevent truncation.PLGPa never floods and its packet forwarding overhead is favourable. It demonstrates more equitable routing load distribution and path diversity. Even without hardware, the cryptographic computation required for PLGPa is tractable even on 8-bit processors.



VII. RESULT

A. Data Set –

1) DBLP Data Set–

DBLP dataset maintains a collection of computer conference journals, papers and proceedings. It has a collection of more than 2.3 million articles with their information like author, title of the paper, link to author's home page, etc.

2) Result Set-

Since the system is in design and implementation phase it is assumed that the system will perform better than the traditional approach. The performance of the search on any dataset can be monitored by any user within the system.

VIII. RESULT SET

Results show that depending on the location of the attacker, network energy expenditure during the forwarding phase increases from between 50 to 1,000 percent and also proposed defences against some of the forwarding-phase attacks and PLGPa that bounds damage from Vampire attacks by verifying packets.

IX. CONCLUSION

This paper defined Vampire attacks also known as a new class of resource consumption attacks that use routing protocols to completely disable ad hoc wireless sensor networks by reducing battery lifeof nodes. These attacks do not rely on specific protocols or implementations instead of it exposes vulnerabilities in a number of well-known protocol classes. They also have shown a number of proof-of-concept attacks against existing routing protocols using a less number of weak attackers, and determined their attack success on topology of 30 nodes. Depending on the location of the attacker, network energy expenditure during the forwarding phase increases. Authors proposed defences against some of the forwarding-phase attacks and described PLGPa.By checking that packets consistently make progress toward their destinations, the first sensor network routing protocol that bounds damage from Vampire attacks .

X. FUTURE SCOPE

Ad hoc wireless sensor networks promise exciting new applications in the near future. As WSN's become more and more crucial to everyday life availability faults become less tolerable. Thus high availability of these nodes is critical and must hold even under malicious conditions.

ACKNOWLEDGEMENT

The author would like to thank Prof. Devendra Vatsa for his help. This work was supported in part by the JDCT, Indore.

REFERENCES

[1] Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly, Denial of service resilience in ad hoc networks, MobiCom, 2004.

[2] Haowen Chan and Adrian Perrig, Security and privacy in sensor networks,Computer 36 (2003), no. 10.

[3] Jae-Hwan Chang and Leandros Tassiulas, Maximum lifetime routing inwireless sensor networks, IEEE/ACM Transactions on Networking 12(2004), no. 4.

[4] Jing Deng, Richard Han, and Shivakant Mishra, Defending against path based DoS attacks in wireless sensor networks, ACM workshop on security of ad hoc and sensor networks, 2005.

[5] Sheetalkumar Doshi, Shweta Bhandare, and Timothy X. Brown, An on demand minimum energy routing protocol for a wireless ad hoc network,ACM SIGMOBILE Mobile Computing and Communications Review 6(2002), no. 3.

[6] Sharon Goldberg, David Xiao, Eran Tromer, Boaz Barak, and Jennifer Rexford, Path-quality monitoring in the presence of adversaries, SIGMETRICS,2008.

[7] Mina Guirguis, Azer Bestavros, Ibrahim Matta, and Yuting Zhang,Reduction of quality (RoQ) attacks on Internet end-systems, INFOCOM,2005.

[8] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, Ariadne: A secure on-demand routing protocol for ad hoc networks, MobiCom, 2002.

[9] ________, Packet leashes: A defense against wormhole attacks in wireless ad hoc networks, INFOCOM, 2003.

[10] Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig, Secure sensornetwork routing: A clean-slate approach, CoNEXT, 2006.

[11] David R. Raymond, Randy C. Marchany, Michael I. Brownfield, and Scott F. Midkiff, Effects of denial-of-sleep attacks on wireless sensor network MAC protocols, IEEE Transactions on Vehicular Technology 58 (2009), no. 1.

[12] David R. Raymond and Scott F. Midkiff, Denial-of-service in wireless sensor networks: Attacks and defenses, IEEE Pervasive Computing 7(2008), no. 1.

[13] Frank Stajano and Ross Anderson, The resurrecting duckling: security issues for ad-hoc wireless networks, International workshop on security protocols, 1999.

[14] Lakshminarayanan Subramanian, Randy H. Katz, Volker Roth, Scott Shenker, and Ion Stoica, Reliable broadcast in unknown fixed-identity networks, Annual ACM SIGACT-SIGOPS symposium on principles of distributed computing, 2005.

[15] Anthony D. Wood and John A. Stankovic, Denial of service in sensor networks, Computer 35 (2002), no. 10.