International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 7.421| Peer Reviewed & Referred Journal |

| Volume 10, Issue 1, January 2023 |

Secure Communication Protocols with Adaptive Topology Control Networks

A.YOGANATHAN, DINESH S

Assistant Professor, Department of Computer Applications (MCA), K.S.R. College of Engineering (Autonomous), Tiruchengode, India

Department of Computer Applications (MCA), K.S.R. College of Engineering (Autonomous), Tiruchengode, India

ABSTRACT: Due to unattended nature of wireless sensor networks (WSNs), an adversary can capture and compromised nodes and made attacks which permanently disable networks by quickly drain the nodes' battery power. Prior security work in this area has been focused on denial of communication. In this paper, a clean slate routing protocol called PLGPn is proposed, which presents a various mechanisms of resource depletion attacks. This mitigates the various types of attacks by improving an already existing protocol called PLGPa. These are clean slate routing protocols capable of overcoming problems such as carousel attack, stretch attack, directional antenna attack and malicious discovery attack during topology discovery phase. Developing such mechanisms is used to avoid the looping among the nodes in the network by loop-free technique. This scheme provides defence for topology discovery and avoid looping concept in an efficient and robust manner even if there are a large number of active attackers in the network.

KEYWORDS: Denial of service; clean slate routing; wireless ad-hoc networks; PLGPn; topology discovery.

I. INTRODUCTION

Ad hoc wireless sensor networks (WSNs) promise exciting new applications in the future technologies as low power sensing device, military appliances. As WSNs become more and more crucial to the everyday functioning of people and ad-hoc based networks does not need any central admin and its setup cost is low, these are used in wide range of applications. But there is a huge availability of these networks is a critical property, and should hold even under malicious condition. The goal of this work is to ensure node-to-node message delivery, even if the sensor network is in unsecure condition. In the presence of an attacker, it is an extremely challenging task to maintain correct routing information; the attacker could inject malicious routing information or alter legitimate routing paths. Routing protocols are providing an optimal data transmission route from sensor nodes to sink to save energy of nodes in the network.

These sensor nodes have a critical piece of information to be sent to the sink. Therefore reliable sensor-to-sink communication has to be guaranteed for such areas. This is the main concept of the various issues and strategies of reliable communication in this paper. There are three main subjects for designing secure routing protocols: *prevention*, *detection / recovery*, and *resilience*. The *prevention* approach is done by cryptographic mechanisms that restrict attacker's actions. *Detection* involves monitoring behaviour of protocol functions. Once malicious behaviour is detected, we need to recover it. The *recovery* techniques eliminate attackers and to restore the network actions. The *resilience* approach seeks to maintain a certain level of availability even there is as failure. Previous secure routing protocols usually rely on a single approach. It is effective against known attacks; an example is the S-BGP protocols [3],the watchdog scheme attempts to identify malicious behaviour in ad hoc networks [5], and secure routing mechanisms attempt to find out malicious nodes along a routing path [7].To mitigate attacks during packet forwarding phase PLGPa protocol[1] is examined.

Adversary can target not only the forwarding packets but also route paths and topology discovery phases. In our routing protocol, we dynamically establish routing tables and full path history at each node using techniques that prevent attacks. We then apply routing techniques to transmit packets, while incorporating mechanisms to detect and eliminate malicious nodes. The memory overhead for our routing protocol is low, each sensor node stores one routing entry for each prefix of its address, representing the next-hop neighbour node to move towards the destination area. Then damage bounds and defences for topology discovery are derived using various mechanisms.

Routing protocols may be divided into two types: proactive and reactive protocols. In a proactive protocol, nodes are periodically transferring the routing information. In a reactive (on-demand) protocol, the information about the routing is shared only when there is a need for it. Each kind of routing protocol has some prons and cons. In this paper, we concentrate secure ad-hoc clean slate routing protocols and in particular with proposed PLGPn protocol. This protocol is efficient in terms of; it saves the (energy) battery power of the network. There are numerous protocols such as SEAD, ARAIDNE are defined but none of them is used to save the power consumption, rather it focus on to save the node itself in the network. In this paper, we present a series of increasingly damaging malicious attacks, evaluate the vulnerability of several protocols, and suggest how to improve protection during topology discovery phase.

In Section II of this paper, we discuss the various related works. In Section III, we describe the basic operations of clean slate routing, and we describe PLGPa wireless ad-hoc sensor network routing protocol on which we consider as our basic work. In Section IV, the possible attacks against PLGPa protocols are specified. In Section V, we proposed a protocol called PLGPn, our modified clean slate routing protocol and compare it with the basic PLGPa protocol. In Section VI, system model is defined. The rest of the paper shows the conclusion.

II. RELATED WORK

In [9, 10], INSENS provides routing between nodes and base stations, but not between arbitrary sensor nodes (except by relaying through the base station). In contrast, we design a general secure routing protocol that can relay messages between arbitrary nodes.

Karlof and Wagner describe attacks on standard (unsecured) sensor network routing protocols and propose some generic countermeasures, without proposing a complete protocol [15].

S.Sarjoun Doumit and P.Dharma Agrawal proposed that the two nodes use an out-of band channel (e.g., a directional antenna) to forward traffic between themselves enabling them to mount other attacks [13].

M. Poturalski et al. proposed that a malicious node creates multiple fake identities to perform attacks. In this, protocol [16] fake identities can claim to be at the multiple locations. V. Gligor et al., proved that an adversary may compromise a single legitimate node and insert copies throughout the network increasing their presence in the network and thus allowing them to influence and subvert the network's performance [17].

In other work, a secure routing protocol for ad-hoc networks namely Araidne [12], which provide security for end-to-end delivery, and SEAD [4] which works as hop-by-hop for distance vector routing but the path control is absent in these distance vector routing protocols. DoS attacks and its resistance mechanisms are briefly mentioned in [2], [8], [9], [14].These mechanism are only give resist on the DoS specific attacks with replay resistance[10] and does not consume the energy and resources.

Y.Eugene Vassermann and Nicholas Hopper [1] proposed a protocol called PLGPa, the first sensor network routing protocol that provably bounds damage from vampire attacks by verifying the packets towards the destination. . This prevents Vampire attack which means creating and sending messages by malicious node which causes more energy consumption by the network leading to slow depletion of node's battery power. This attack is not specific to any protocol; instead it uses protocol complaint messages. Few kinds of attacks are carousal and stretch attack. It derives the damage occur during packet forwarding phase but instead we modified the protocol as PLGPa which prevents the node in the network during topology discovery.

III. CLEAN SLATE ROUTING-PLGPa

The clean slate secure sensor network routing protocol called PLGPa can prevents various types of attacks during the packet forwarding phase. It has two phases as topology discovery phase and packet forwarding phase.

A. Topology Discovery

There may be different types of topology construction. But it should be discovered at a time limited period. Nodes need to join as a group. Each node stores the virtual address of other nodes in the network. These nodes build a tree like structure for neighbouring relationship. Discovery phase makes the nodes to create a tree, which is turn into addressing scheme for that network. Then the nodes are needed to discover the neighbours and create a neighbourhood which forms a network as a group. Then the multiple groups are created in multiple locations.

B. Packet Forwarding

In this phase, each node made decisions independently. While forwarding the packets, it is necessary to shorten the distance to the destination.

IV. ATTACKS ON PLGPa

In this kind of protocol, the nodes which are forwarding the packets do not know where the path to send a packet is. This allows the malicious attackers to divert the packets to any false locations in the network. This makes the PLGPa vulnerable to attacks. Thus, in this way the attacker moves the packet away from the destination. The attackers are not able to do attacks on nodes, rather it rely on route specified by the source. We examined two types of attacks that affect this protocol PLGPa. They are carousel attack and stretch attack.

A. Carousel Attack.

In this type of attack, an adversary composes packets with purposely introduced loops between the nodes. This is named as carousel attack, since it sends packets in circles. It targets source routing protocols by exploiting the limited verification of message headers at forwarding nodes, by making a packet to travel along the same node as many times. This attack is mentioned in various literatures, but neither intuition for defences nor any evaluation is provided. In this attack, an adversary sends a packet with a route composed as large loops, such that the single node appears in the route as so many times. This is the method of adversary to increase the route length beyond the number of nodes in the network.

B. Stretch Attack.

In this attack, also targeting source routing, an adversary creates artificially long routes, potentially covered every node in the network. We call it as stretch attack, since it stretches the length of packet paths, 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. A single attacker can use a carousel attack to increase energy consumption while stretch attacks increase energy usage by up to an order which depend upon the location of the malicious node.

C. Methods to preventing the attacks.

In carousel attack, the packet is rerouted again and again. The original length of the route is disrupted and bounded by damage, so the packet can create a cycle in indefinite manner. But it can be avoided by forwarding node which needs to check the source routes for loops or simply drop the packets without allowing them to pass through the network. The stretch attack may be avoided by loose source routing. In this the intermediate nodes may replace a part or the entire route in packet header, if they know a better alternate route to destination. But this the challenging task. In this case, it needs to cache the best routes to forwarding the packets. But it is not obvious than the global topology network. Therefore there is need for modifications in the packet forwarding phase of this existing PLGPa protocol.

V. PLGPN-MODIFIED PLGPA PROTOCOL

In this section we modify the PLGPa protocol as PLGPn. It is the first sensor network clean slate routing protocol which prevents the Vampire attacks, and automate the messaging system. This prevention is by checking the movement of the packet towards the destination. It securely governs the progress of an each packet and also provides no-back warding property. This property states that the movement of each node does not need to go backwards for any satisfactory process.
This protocol prevents the types of attack as carousel and stretch attack and thus avoids looping by sending through the specified path.

A. Basic Design of PLGPn

Here, we start the basic design of PLGPn, the clean slate routing protocol on with the bass of PLGPa. In contrast to PLGPa, to avoid the looping concept in PLGPa, we use the mechanism as forwarding nodes are needed to check the loops or just simply drop the packet. This is the way to avoid the carousel attack. For stretch attack, the source routing must be maintained. Instead of using strict source routing, we use loose source routing to avoid the alteration in the packet route length, in which if the intermediate nodes knows a better route to destination, it will replace a single route or the entire route of the packet. But this strategy of recovery needs more energy to spend on the packet routing.

PLGPn differs from PLGPa in the way that maintain the energy saving and also no-back warding property. This is the property, in which the nodes are no need to check for the originator authorization every time. In this PLGPn, the packet progress is securely verified towards the final sink in the network. The back warding property is satisfied, only when the number of hops covered by the honest node and the malicious node is same. So, the energy usage is also common.

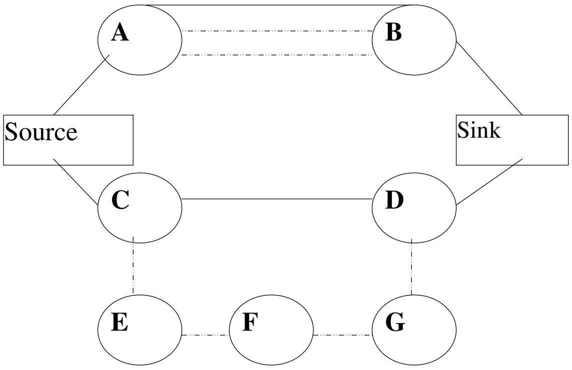

Fig. 1 PLGPn System Architecture

- Solid Lines are honest path where dotted ones are attacker path.
- B, E, F, G are attacked node by an adversary.

In this scheme, every packet is attached with attestations. This attestations content is filled with the full packet path history. This path history is secured by the originator. These attestations are grouped together. Because of all the attestations are combined and chained together, the path history is verified securely, therefore the attacker are not able to compromised any node because the packet must travel along anyone of the valid honest node. If there is any adversary in the network, only the attestations are hacked and damaged, and not the full packet because every packet are signed by the original authenticator. With PLGPn, there is no way for looping to occur in the network. This is attained by, the path are discovered at initial topology discovery time itself. Unlike, other protocols, the full path history towards the sink node is set in advance. Each and every node is filled with the entire path history.

If any adversary in the network tries to damage the packet, it really gets the attestations attached with the packet and not the packet or node. So, there is nothing to gain in damaging the attestation because each and every packet are securely verified and authenticated by the originator. This is the better choice to avoid looping among the nodes. The major concern of this paper is to reduce the energy usage in the network. So, if the path history is set in advance, there is no need to packet progress rediscovery. Once the malicious node is detected, it may be punished or not allow to enter into the network again. This is meant by if there is a node which created loop in the network, it just discarded. Therefore, the energy automatically saved. This strategy does not exist in PLGPa protocol. The comparison of PLGPa and PLGPn protocol as described below in Table 1

PLGPn PROTOCOL	***PLGPa PROTOCOL***
Defence attacks during topology discovery phase.	Defence attack during packet forwarding phase.
Prevents attacks on long-term availability.	Prevents attacks on short-term availability.
PLGPn brings the better performance in both state full and state-less protocols.	Works better only in stateless protocols.
This satisfies the no-back warding property and also avoids looping among the routes.	This protocol does not satisfy no-back warding property and thus creates loops.

TABLE 1- Comparison of Proposed (PLGPn) and Existing (PLGPa) Protocol

B. Neighbour Relationship

The neighbour of each node in the network is authenticated in PLGPn. If the neighbour is not an authenticated node, looping is created by them itself. The mechanism such as TESLA [6] is used to neighbour authentication, but there is a pitfalls in these approaches, that is it needed a time synchronization to maintain the neighbour relationship. To authenticate the neighbour relationship in the network, we use PLGPa [1] mechanism to discover the neighbourhoods. At the discovery phase itself, each node creates its own neighbouring node by itself. All the nodes in the network know the neighbour's node virtual addresses and authenticated keys. Each node maintains the neighbour authentication in the way that forming a group together. If the receiving node is not a neighbour, discard the packet.

```
Function secure_forward_packet(p)
s —— extract_source_address(p);
a —— extract_attestations(p);
if(not verify_source_sig(p))
then
return;    /*Discard the packet*/
foreach node in a do
prevnode —— node;
if(not are_neighbors(node,prevnode))
then
return;   /*Discard the packet*/
c —— closest_next_node(s);
p'___ saowf_append(p);
if  is_neighbors(c) then forward(p',c);
else forward(p',next_hop_to_non_neighbor(c));
```

C. Defending the Topology Discovery

The topology discovery phase is considered as the initial main phase in the network construction. There is a need to synchronize the discovery. In this topology discovery phase, all the discovery terms is introduced. The certification of each node is given in this phase. Every message is signed by the authorized sender. The major issue in this is that the malicious node creates flooding, merging of the nodes and thus cause looping. This creates a serious problem. Therefore we need to provide more security on topology.

In PLGPn, at the initial setup, first the node is allowed to send through the network. It finds out the shortest distance using the implementation of the Bellman-ford algorithm. Then, consider it as the honest path. So each and every node allowed to forming a group with the full packet history. Therefore, there is no way to alter the path like creating loops and lengthen the path such as carousel and stretch attack. If there is a malicious insider in the network, the node's path does not altered, only it able to damage the attestations and there is no use in it, because other nodes are able to maintain the path. To prevent the Vampire Attacks in Topology construction, the following steps are followed.

Finding the Shortest Path

PLGPn computes the shortest path between the nodes by the Classical Bellman-Ford Algorithm. This algorithm is very efficient when solving the single source related problem, if there are large weights in the node.

.

Loop-free Technique

Once the shortest path is known, data packets are shared through that path and check for loops. To avoid the loops created by the malicious, we use this loop-free technique. This is the technique for checking loops created in the routing path. While transferring the packets to other nodes, first allow to send through the computed shortest path. Only, in accordance with topology constructed, the paths are maintained.

If there is a node which makes a false claim about discovery, just discard the node to again participate in the network. The nodes are travelled through the specified path at only one time. The next time, there is another way to send the packets. Because, the loops are created here by the honest node itself, the packets are sending through other nodes in the network. Therefore, just discard the node which creates a loop. For e.g.: Consider Fig 1. The shortest path computed at first time is ABC means, allowed to send through this path. The second time it shows the path as CDE means, here node C created a loop in the network. So, just discarded the node C to participate in the network.

D. Handling Mobile Networks

In ad-hoc sensor networks, handling the mobile networks is the challenging one. In PLGPa, we give some intuitions to handle the Vampire attacks in mobile networks. There are some steps while handling the mobile ad-hoc routing networks as described below.

1. Register to the network for authentication.
2. Ask key for transmission and compute the shortest distance among the mobile nodes.
3. Transmit the packet through the shortest path specified.
4. Check for loops using Loop-free algorithm.
5. Do the verify process.
6. If it is honest one, accept the message or just discard it.

But in mobile ad-hoc networks, the attackers may able to do attack by using directional antenna method to capture the neighbouring nodes. This leads to merging of the nodes. In malicious discovery attack, the malicious may act as a neighbour of the honest node and make a fool the honest node. This is the powerful attack to discover. In these mobile networks, the attacker may less punish in malicious discovery attack. And also of using the full path history in the every single packet, the packet size may increase.

V. SYSTEM MODEL

I. Topology Construction Module

In this module, first the user needs to authenticate. User needs to register their details to sending a packet or a message. Then the topology designs of the network are constructed. These are constructed in the way that, there are two paths to verify the honest one. If the user details are correct, the node message is showed in the honest path. Otherwise it placed in the malicious path. The same criteria is also used in the receiver side

B. Denial of Service Module

Denial of service is an attempt to make the system resources unavailable to the responsible user. This is the system to interrupt the main services. In this, we should consume the resources to avoid denial of communication by strictly authenticate the entire network.

C. Data Verification Module

This module consists of verification of data and its integrity. This is the phase that done in receiver side. Here, the receiver verifies the path. This shows that if the data are passed through the attacker path, it will place in malicious path or else it will place in honest path. Otherwise it placed in honest packet. This module is concentrate on data accuracy and consistency.

D. Carousel Attack Module

This is the module for looping elimination. In this we use a loop-free technique. This technique is used only to allow the permitted node. Here the nodes are allowed to check for looping in their path. Once it detected the node which is responsible to create a loop, is discarded. And that node is not allowed to enter into the transmission process again.

E. Stretch Attack Module

The malicious node creates a long route to increase the original path length. It will affect the entire nodes which are participated in the network. The neighbouring nodes are check for original path. If one node fails, the other nodes are able to retain the original path and reach the destination. This is the main module to concentrate on attack prevention. In this module, the attackers' entry is detected.

VI. CONCLUSION

Providing energy saving and resource management schemes in wireless sensor networks (WSNs) is an efficient thing in case of various attacks. In this paper, we defined a new resource management protocol PLGPn, to mitigate attacks of Vampire such as Carousel and Stretch attack. We proposed a secure routing protocol providing solution for energy conservation. This PLGPn protocol provides the defences of topology and consistently gives security during packet forwarding phase by selecting the preferred shortest path. This is the full satisfactory solution for Vampire attacks like stretch attack and carousel attack. We give some ideas to further improvement on PLGPn.

In future work, we plan to derive the damages on malicious discovery and directional antenna attack and to reduce the packet size in case of maintain of bandwidth efficiency.

ACKNOWLEDGEMENT

We would like to thank our management, Principal, and Dept. staff members for providing this environment and special thanks to Salem Jeyaseelan for his guidance, and our anonymous reviewers for their valuable and helpful comments and suggestions for this paper.

REFERENCES

1] Y.Eugene Vassermann and Nicholas Hopper, "Vampire attacks: Draining life from wireless ad-hoc sensor networks", *Proc.IEEE Transactions on Mobile Computing*, vol. 12, no. 2, pp. 318-332, February 2013.

2] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," In Proceedings of. 12th Conf. USENIX Security, 2003.

3] S. Kent, C. Lynn, and K. Seo, "Secure border gateway protocol (S-BGP)", *IEEE Journal on Selected* Areas in Communications, 18(4):582-592, Apr. 2000.

4] 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

3] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks",In Proceedings of ACM Mobicom, pp 255-265, Aug. 2000.

4] Adrian Perrig,Ran Canetti,Dawn Song, and J.D Tygar, "Efficient and Secure Source Authentication for Multi-cast", *In Network and distributed System Security Symposium(NDSS'01)*, February 2001.

5] V. N. Padmanabhan and D. R. Simon, "Secure traceroute to detect faulty or malicious routing", *SIGCOMM, Computer Communication Review (CCR)*, pp. 77-82, 2003.

6] I. Aad, J.-P. Hubaux, and E.W. Knightly, "Denial of Service Resilience in Ad Hoc Networks," *In Proceedings of* ACM *Mobicom*, 2004.

7] J. Deng, R. Han, and S. Mishra, "INSENS:Intrusion-tolerant routing for wireless sensor networks", *Elsevier Journal on Computer Communications, Special Issue on Dependable Wireless Sensor Network*s, 2005.

8] Tuomas Aura, Dos-resistant authentication with client puzzles, *International workshop on security protocols*, 2001.

9] J. Deng, R. Han, and S. Mishra, "A performance evaluation of intrusion-tolerant routing in wireless sensor networks", *In IEEE Workshop on Information Processing in Sensor Networks (IPSN)*, pages 349-364, Apr. 2003.

10] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks" *In Proceedings of ACM Mobicom,* Sept. 2002.

11] S.Sarjoun Doumit, P.Dharma Agrawal, "Self-Organizing and Energy-Efficient Network of Sensors", *In Proceedings of MILCOM Distributed & Mobile Computing,* pp. 1-6, 2002.

12] 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.

13] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", *Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols*, 1(2-3):293-315, Sept. 2003.

14] M. Poturalski, P. Papadimitratos, and J.-P. Hubaux, "Secure Neighbor Discovery in Wireless Networks:" Formal Investigation of Possibility," *Proc. ACM Symp. Information, Computer and Comm. Security* (*ASIACCS),* 2008.

15] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks", *In Proceedings of IEEE Symposium on Security and Privacy*, May 2005.

16] T. English, M. Keller, K.L. Man, E. Popovici, M. Schellekens, and W. Marnane, "A Low-Power Pairing-Based Cryptographic Accelerator for Embedded Security Applications," *Proc. IEEE Int'l SOC Conf.* , 2009.

17] L.B. Oliveira, D.F. Aranha, E. Morais, F. Daguano, J. Lopez, and R. Dahab, "TinyTate: Computing the Tate Pairing in Resource- Constrained Sensor Nodes," *Proc. IEEE Sixth Int'l Symp. Network Computing and Applications (NCA*), 2007

18] A. D. Wood, L. Fang, J. A. Stankovic, and T. He. SIGF: A family of configurable secure routing protocols for wireless sensor networks. *In Proceedings of ACM SASN*, Oct. 2006.