Weakening the Intruders using PLGP in Wireless Adhoc Sensor Networks

J. K. JayaKumari[1] P. Srinivasaragavan[2]
[1] PG Student[2] Assistant Professor
[1, 2] Computer Science Engineering
[1, 2] P. S. R. Engineering College, Sivakasi, India

Abstract---An exhilarating research area in sensing and pervasive computing is ad-hoc low-power wireless networks. Sensor networks pose a number of challenging conceptual and optimization problems such as location, energy consumption, and tracking. Vampire attack is a new class of resource consumption attacks in wireless sensor networks. Denial of communication at the routing or media access control level has been focused in the area of prior security. This proposal discovers resource depletion attacks at the routing protocol layer. The attack permanently stalls the network by quick exhausting battery power of the nodes. These vampire attacks do not rely on specific protocol but suitable on different popular classes of routing protocol. The problem examined is many protocols suspected to vampire attacks, which are stealthy to detect and easy to execute with any compromised user who is sending only protocol compliant messages. Due to the shortcomings in the Ariande, SAOD and SEAD do not protect against the attacks. This lead to the emerge of sensor network routing protocol PLGPa. PLGPa is used to reduce the damage caused by vampire attack. This protocol decreases the energy consumption and depletion of resources.

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

I. INTRODUCTION

A new emerged technology using sensing and enveloping computing is Ad hoc wireless networks. An ad hoc network typically refers to any set of networks where all devices have equal status on a network. The concept is Mobile communicates directly with access points. The advantage of ad hoc networks is ease of deployment speed of deployment decreased dependence on infrastructure. A collection of two or more devices equipped with wireless communications and networking capability supports anytime and anywhere computing. The characteristic of ad hoc network are

- Each mobile host acts as a router
- Supports peer-to-peer communications
- Supports peer-to-remote communications
- Reduced administrative cost
- Ease of deployment

In this work, I consider only wireless networks capable of operating without the support of any fixed infrastructure. I also consider the general case of multi-hop networks. More precisely, I will consider wireless ad hoc networks as well as wireless sensor networks.

Typically the base stations are deployed to provide ubiquitous coverage to all mobile nodes at all locations in the network. When the base stations are so close to provide seamless coverage to all areas served by the network operator.

Compatible to 802.11b. In general, the coverage area of a wireless LAN is very small. As users roam in space they are intermittently connected to a local access point. When the access points are far apart and the pockets of coverage areas are disjoint. Infostation networks, pioneered by researchers at WINLAB are a conceptual departure from the ubiquitous (anytime/anywhere) assumption in conventional cellular services. It is motivated by the fact that data services are often connectionless, delay insensitive, and have no specific bit rate requirements By restricting the transmit range of an infostation to the locality when the channel condition is excellent, the capacity is optimized from an information theoretic perspective. For nodes with low mobility, the infostation network is akin to a wireless LAN as depicted in with high bit rate islands of coverage close to the infostations. However, a wireless LAN typically does not support node mobility. To date, different access points have different ownership and operate autonomously without coordination or cooperation. The sharing of access points for roaming users is largely prohibited. An infostation network calls for the explicit co-ordination of infostations as a user moves around. A user may download parts of a large file from different infostations as it roams around the network in due time. The second paradigm in wireless networking is mobile ad hoc networks, which includes multihop ad hoc networks and mobile infostation networks. The concept of multi hop networks is not new. In the past two decades there were researches in packet radio networks under the DARPA program, which is an in fact multihop network with a fancy name. On the other hand, the idea of mobile infostation networks very recent, inspired by the infrastructure infostation networks. Although there are no large scale commercial deployment of these two networking paradigms to date, it is undeniable ad hoc networks are becoming one of the most active areas of networking research in these few years. A casual search in the ad hoc network literature reveals that there are very few papers in ad hoc network in the year 1997. Since then, the subject of ad hoc networks has captured the attention of many researchers

The diversity of the applications supported by wireless ad hoc and sensor networks explain the success of this type of network. These applications concern as various domains as environmental monitoring, wildlife protection, emergency rescue, home monitoring, target tracking, exploration mission in hostile environments, etc. However, the most critical requirement for adopting such networks is energy efficiency. Indeed, some nodes are battery operated and battery replacement can be difficult, expensive or even impossible. The goal of communication protocol designers is then to maximize the lifetime of such networks.

A. Specificities of wireless ad hoc and sensor networks

Wireless ad hoc and sensor networks have in common some characteristics that have to be taken into account by energy efficient techniques:

- *Lack of pre-configuration:* A wireless ad hoc and sensor network is a collection of wireless nodes that can dynamically self-organize into an arbitrary and temporary topology to form a network without using any pre-existing infrastructure.
- *Wireless communication:* which has the following properties:
- *Radio interferences:* Indeed, when a node N1 is transmitting to a neighbor node N2, no other node in the transmission range of N1 can receive another frame. Similarly, no other node in the transmission range of N2 can send another frame.
- *Radio link versatility:* as the propagation conditions change very frequently, the quality of a radio link varies strongly in the time.
- *Limited bandwidth:* the wireless bandwidth has a capacity much smaller than a wired one due to the shared nature of the wireless channel and interferences.
- *Scalability:* Communication protocols should be able to support large (i.e. a high number of nodes) or dense (i.e. a high number of neighbors per node) wireless networks.

B. Differences between wireless ad hoc and sensor networks

While wireless sensor networks share many commonalities with existing ad hoc network concepts, there are also a number of differences and specific challenges applications. The main difference between common ad hoc networks and wireless sensor networks is their different area of application. In fact, a sensor network is characterized by its strong interaction with its environment. For this reason, it can be used in a large number of applications like

- Indoor/outdoor environment monitoring
- Monitoring of buildings/bridges/airplanes for structural integrity
- Ubiquitous computing for healthcare applications
- Sensing within factory environments
- Sensing for transportation applications
- Warehouse and retail inventory management
- Interactive museums/exhibits, etc.
- Constraints. Constraints in wireless sensor networks are stronger than in ad hoc networks because of the miniaturization of sensor devices
- Limited memory/storage.
- Limited processing capacity.
- Radio transceiver: the radio range is generally shorter (20m in 802.15.4 versus 250m in 802.11b).
- Low rate: 250 kbps in 802.15.4 versus 11Mbps in 802.11b.
- *Limited energy:* The energy constraint in wireless sensor networks is stronger than in ad hoc networks. This is because, sensor networks are usually deployed in hostile environment or the number of nodes in the network can be very important.
- *Mobility support:* It is an evident requirement for VANETs (Vehicular Ad hoc Networks), for instance. It is usually not required in many wireless sensor networks: in these networks, either all nodes are fixed or a very limited number of them are allowed to move.

The main work on this process is based on the routing or medium access control levels according to the rejection of communication in a network. There are various kind of attack based on that only routing protocol is developed. The intruder in the network can able to disable the whole networks by quickly draining nodes' battery power. The main disadvantage is a single node can increase network-wide energy usage and make the other node weaken. I construct an advanced protocol based on the damage caused by intruder during the packet communication path.

II. RELATED WORKS

As Reviewed in[1] A major concern about distance-vector routing protocols for wireless mesh networks is its slow convergence in the presence of link changes, which can potentially degrade network stability. This paper studies the impact of update intervals on network convergence. It is studied with a combination of model-based analysis and simulation-based performance evaluations. A fast converging distance-vector routing algorithm is proposed to improve route convergence speed. Here simulation results have shown that the proposed algorithms could effectively reduce convergence latency, improve routing throughput without leading to a significant increase in control overhead. Existing routing protocols (including link-state routing, on-demand routing and source routing) tend to broadcast network-wide control messages in order to discover and maintain routes between end nodes. Therefore, these protocols can have high a message overhead when used in WMNs. Distance-vector routing protocols like DSDV, however it have a lower overhead since the nodes running distance-vector protocols only exchange control messages with their adjacent nodes.

As Reviewed in[2] Routing is one of the most basic networking functions in mobile ad hoc networks. Hence, an adversary can easily paralyse the operation of the network by attacking the routing protocol. This has been realized by many researchers and several secure routing protocols have been proposed for ad hoc networks. However, the security of those protocols has mainly been analysed by informal means only. In this paper, flaws in ad hoc routing protocols can be very subtle and a more systematic way of analysis. Mathematical framework is proposed in which security can be precisely defined and routing protocols for mobile adhoc networks can be proved to be secure in a rigorous manner. Some framework is tailored for on demand source routing protocols, but the general principles are applicable to other types of protocols too. This approach is based on the simulation paradigm, which has already been used extensively for the analysis of key establishment protocols, but, to the best of our knowledge, it has not been applied in the context of ad hoc routing so far. Here a new on-demand source routing protocol is proposed, called endairA and demonstrate the use of our framework by proving that it is secure in the model.

As Reviewed in[3] In this paper, a protocol is presented for monitoring packet-loss rates that makes extremely efficient use of communication and storage resources. Secure sketch protocol uses 2-norm estimation sketches to aggregate information about the failures that occur during an interval, in which T packets are sent, into a sketch of size O(logT) bits. The communication overhead is just a single report packet per time interval. This paper emphasizes that a PQM protocol does not prevent failures. A secure PQM protocol achieves its goal even when there is an intermediate node on the path between source and destination that can frequently drop, modify, or inject both data and protocol-related packets to the path in order to bias the measurement results. Most existing PQM protocols, such as ping, trace route, and counter-based solutions completely break down in this setting.

As Reviwed in[4] As mobile ad hoc network applications are deployed, security emerges as a central requirement. In this paper, the wormhole attack is introduced, a severe attack in ad hoc networks that is particularly challenging to defend against. The wormhole attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them there into the network. The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols and location-based wireless security systems. For example, most existing ad hoc network routing protocols, without some mechanism to defend against the wormhole attack, would be unable to find routes longer than one or two hops, severely disrupting communication. A new general mechanism is presented and it is called packet leashes. It is used for detecting and thus defending against wormhole attacks, and presented a specific protocol called TIK, that implements leashes.

III. SYSTEM DESIGN

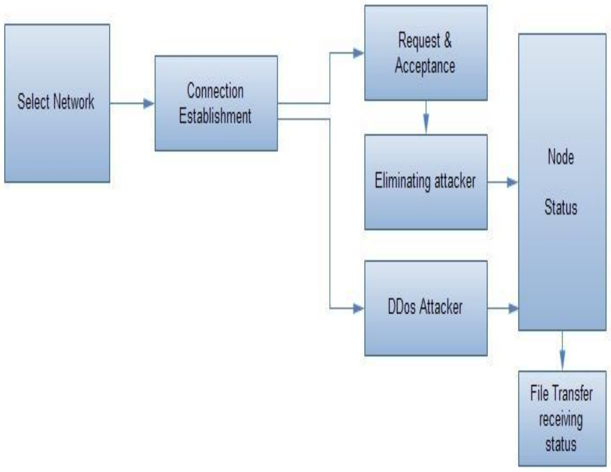
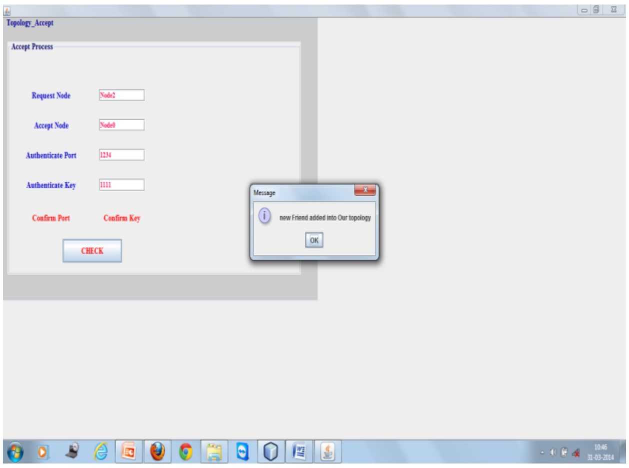


Fig. 1: Architecture

IV. RESULTS



Request Node Node2

Accept Node Node0

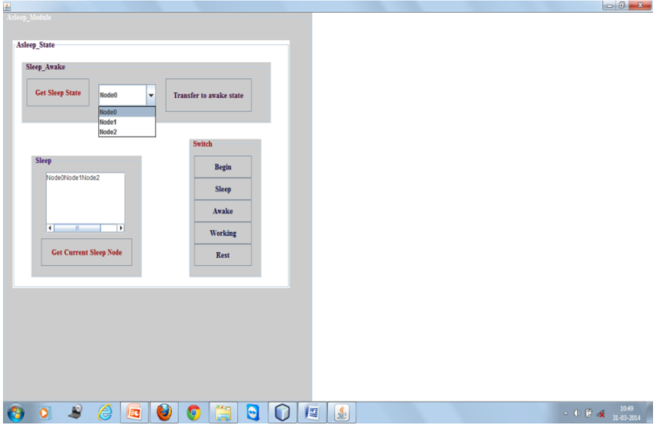
Authenticate Port 1234

Authenticate Key 1111

new Friend added into Our topology

Fig. 2: Trusted Topology Process

In this module a new wireless network is formed. Getting the number of nodes for adding into wireless network from the users. Getting the radius level which is being covered by each node. Finally forming a wireless network and establishing the communication for all nodes. I have formed a Initial topology structure. In this module II am forming a trusted topology. Choose a Node For that want to join trusted topology. Requested Node must be Submit a policy which is requiring a trusted node. Choose a Node for grant Permission for requested node which is already joined the trusted topology. For forming trusted topology PLGP protocol is used. Accept Node must be check the require policy which is submitted by Requested node. From this process, the outsider attack can be filtered from our topology. Now the topology keeps safe from the outsider attack. Meta protocol have many states that is Begin state, Sleep state, Awake state, Rest state, Working state and halt state. Begin state is initial state for all the nodes which is joined into topology. All the nodes should be shift from begin state to sleep state. The node which is stay into sleep state that can shift to awake state. The Awake state nodes may shift to either working state or back to sleep state. Working state nodes only can transfer the files between them. Working state nodes may be shift to either rest state or back to awake state. The rest state nodes can move to either sleep state or return to working state. Thus the power consumption of nodes can be reduced.



Node0

Node0Node1Node2

Fig. 3: State of each nodes (Begin state, Sleep state, Awake state, Working state, Rest state)

V. CONCLUSION

I 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. Authentication and Dos attacks come in the category of this attack. Here in this phase I have measured and showed the results, to elimate the outsider attacks(authentication attack) and improving our battery power by changing the state of each node.

REFERENCES

[1] "Vampire Attacks: Draining Life fromWireless Ad Hoc Sensor Networks", Eugene Y. Vasserman and Nicholas Hopper,2013.

[2] 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.

[3] S. Goldberg, D. Xiao, E. Tromer, B. Barak, and J. Rexford, "Path- Quality Monitoring in the Presence of Adversaries," Proc. AC SIGMETRICS Int'l Conf. Measurement and Modeling of Computer Systems, 2008.

[4] Y.-C. Hu, D.B.Johnson, and A.Perrig, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks", Proc. IEEE INFOCOM, 2007.

[5] G. Acs, L. Buttyan, and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 5, no. 11, pp. 1533-1546, Nov. 2008.

[6] 2.5 A. Saxena and B. Soh, "One-Way Signature Chaining: A New Paradigm for Group Cryptosystems," Int'l J. Information and Computer Security, vol. 2, no. 3, pp. 268-296, 2008.