International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Defending Against Source Routing Attacks in Wireless Ad-Hoc Networks

Srihari Babu Kolla[1*], B. B. K. Prasad[2]

[1]M.Tech, Dept. of Computer Science & Engineering, Dhanekula Institute of Engg & Technology, India
[2]Associate Professor, Dept. of Computer Science & Engineering, Dhanekula Institute of Engg & Technology, JNTU Kakinada, India

Abstract: ***The prominence of the place of wireless ad-hoc networking is become more crucial to everyday functioning of people. This is due to obvious advantages of wireless networks with ubiquity access and minimal hardware requirements in networks. The Adhoc nature of sensor networks means no structure can be strictly defined. The network topology is always subject to change due to node failure, addition or mobility. Since nodes may fail or be replaced the network must support self-configuration. Routing and data forwarding is a crucial service for enabling communication in sensor networks. Unfortunately, current routing protocols suffer from many security vulnerabilities. The simple attacks are involves injecting malicious routing information into the network, resulting in routing inconsistencies. Simplest authentication might guard against injection attacks, but some routing protocols are susceptible to reply by attacker of legitimate routing messages. Secure delivery of packets to and from the wireless networks is however a major issue in wireless networks. Low power wireless networks are an existing research direction in routing and packet forwarding. In this paper prior security works in this research direction in routing and packet forwarding. In this paper prior security work in this area focused primarily on routing layer exhaustion attacks. We design a novel routing protocol as SRPF. In this protocol we shown energy consumption monitoring algorithm (ECMA) to bounds the damage caused by source routing attacks during the packet forwarding phase.***

Keywords: ad-hoc networking, energy consumption, vulnerability, source routing, security

1. Introduction

In the recent years, wireless Adhoc networking is become more and more crucial to everyday functioning of human life. One of the main reasons is that routing in MANETs is a particularly challenging task due to the fact that the topology of the network changes constantly and paths which were initially efficient can quickly become inefficient or even infeasible. Moreover, control information in the network is very restricted. This is because the bandwidth of the wireless medium is very limited, and the medium is shared. It is therefore important to design algorithms that are robust, flexible, adaptive and self-healing.

In this paper we present the source routing vulnerabilities in the Adhoc networks. The interesting point in the Adhoc networks, the nodes no need to direct communicate with the remaining nodes for sending data, instead they communicate by the indirect communication of individuals through modifying their nature. Several protocols are introduced in recent years to solve source routing attacks. Unfortunately all the existing protocols, not offered a fully satisfactory solution for the source routing attacks during the topology discovery phase. This is the main reason for securing in Adhoc networks are still an open issue and challenge to researchers.

Wireless Adhoc networks particularly vulnerable to DoS attacks [1], in these attacks malicious node can easily join the network and modify or fabricate routing information and impersonating other networks. An unprotected Adhoc routing is vulnerable to these types of attacks. Attacks on Adhoc network routing protocols generally fall into two types those are:

- Routing disruption attacks
- Resource exhaustion attacks

The above described attacks are totally distinct in nature to all Dos attacks. These are mainly based on different parameters like reduction of quality, routing infrastructure attacks they do not disturb immediate availability, but rather these attacks can cause, work over time to entirely deplete network. If malicious injected to node present in the present network it can spends more resources than the normal routing. For example if it use one minute to its own CPU time to cause the adversary to use ten minutes to process. It can consider as the process of routing any packet from source to destination in any multi-hop network; source composes the packet and transmits to the next hop towards the destination, it transmits it further, until it reaches to its destination, consuming resources not only at the source node but also at every node the message moves through. So we must concentrate on the resources using in the network routing our protocol ultimate goal is the minimizing the resources to process the packet forwarding to destination.

2. Overview

In the rest of the paper we discussed about vulnerabilities with the source routing attacks, evaluate it with the existing secure protocol such as PLGP [2], and suggest how to improve security with our protocol. In this section we have shown how to inject a malicious packet to honest node and how it disturbs in the routing process i.e., source can specify paths through the network which are far longer than optimal, wasting energy at intermediate nodes that mention who forward the packet based on the included source route. Finally we shown how an adversary can target not only packet forwarding but also route and topology discovery phase, if discovery messages are flooded, foe can, for the cost of a single packet, it consume energy at every node in the network.

Licensed Under Creative Commons Attribution CC BY

In the first attack foe can inject a packet with purposely introduced looping with same nodes in the routing. It named as "Routing Disruption Attack" shown in fig 1(a), it targets source routing protocols by limited verification methods of packet header at forwarding nodes allowing a single packet to repeatedly travel the same set of intermediate nodes.

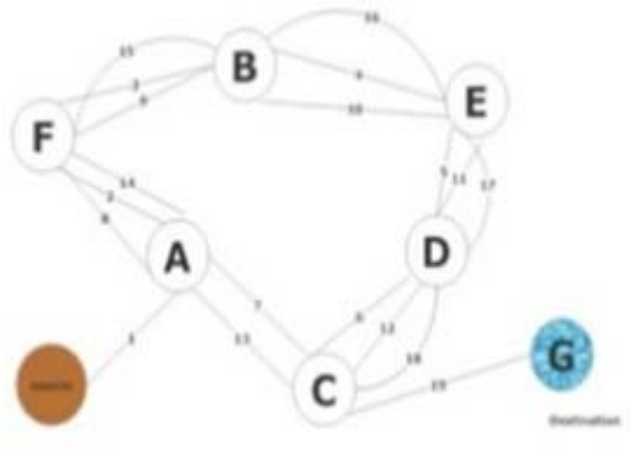


Figure 1 (a): Route Disruption Attack

In the second attack targeting to source routing foe constructs artificially long route than optimal. It causes to traverse every node in the network it is named as "Resource Exhaustion attack" shown in fig1 (b). It can cause to be processed by a number of nodes that is independent of hop count along the shortest path between the foe and optimal destination. In recently there are brief mentions of these attacks can be found in other literature [2, 3], but no intuition for defense or any evaluation is provided.

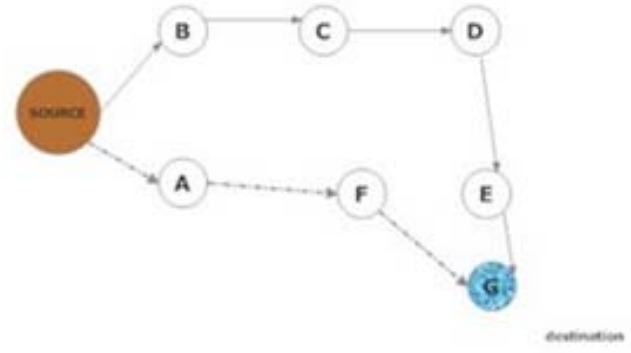


Figure 1(b): Resource exhaustion Attack

Here we described about mitigation for these attacks. The first attack can be preventing, entirely by having forwarding nodes loop in source routes. Of course this checking logic is also more overhead in resources. So when a loop is detected then simply detect that packet. When source intend to send a packet to destination every node must determine the next node by locating itself in the routing. 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 discard that packet. No extra processing is required for this defense, since a node must perform this check anyway; we only alter the way the check is done. Another attack is more risk to prevent. Its successes rest on the forwarding node not checking for optimality of the route. If we call the no-optimization case "strict" source routing, i.e., every packet can traverse as specified in the header. These can e prevent with the loose source routing, in this routing where intermediate nodes may replace a part or all of the route in the packet header if they know of a better route to 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.

3. Background

PLGP protocol is the first sensor network routing protocols that provably bounds damage from vampire by verifying that packets consistently make process toward their destinations. But this not offered fully satisfactory solution for the vampire attacks during the topology discovery phase, but suggested some intuition about damage limitations possible with further modifications to PLGPa. This protocol also not offered fully satisfactory solution for source routing attacks. PLGPa preserves no-backtracking, it is the only protocol discussed so far that provably bounds the ratio of energy used in the adversarial scenario to that used with only honest nodes to 1, and by the definition of no-backtracking PLGPa resists source routing attacks. This is achieved because packet progress is securely verifiable. Note that we cannot guarantee that a packet will reach its destination, since it can always be dropped.

PLGPa includes path attestations, increasing the size of every packet, incurring penalties in terms of bandwidth use, and thus radio power. Adding extra packet verification [4] requirements for intermediate nodes also increase processor utilization, requiring time and additional power.

Other work on denial of service in Adhoc wireless networks has primarily dealt with foe that prevents route setup, disrupt communication, or preferentially establish routes through themselves to drop, manipulate, or monitor packets. Security consideration is the main research to the mentioned. Protocols that define security in terms of path discovery success, ensuring that only valid network paths are found, cannot protect against vampire attacks,, since these attacks do not use or return illegal routes or prevent communication in the short term.

4. Overview of our Protocol

In this section we focus on the design of our protocol. In this, where energy of a node gets to threshold level it plays a vital role by performing energy of the sensors and rendering the network endurable. This protocol based on the two phases. Those are:

1. Network configuration phase.
2. Communication phase.

Licensed Under Creative Commons Attribution CC BY

Network Configuration Phase

In this phase is to establish a optimal routing path from source to destination in the network. The key factors considered are balancing the load of the nodes and minimization of energy consumption for data communication. In this phase the node with threshold level energy (compromised node) sends energy weight (EG_WE) to all its neighbor nodes. After receiving the EG_WE packets the neighbor nodes sends the EG_RPLY message that encapsulates information regarding their geographical position and current level. The node upon receiving this stored in its routing table to facilitate further compositions.

Now the node establishes the routing path, first it checks the neighbor node by computing the energy required to transmit the required data packet that is suitable energy node and less distant node selected as the next forwarding node in this way it establishes the route from source to destination with suitable energy and less distant. Thus energy spent by the allotted node suitable to the data packet sent from the node in this way algorithm avoids data packet dropping and this allotted forwarding node transmits the packets safely to the destination. This algorithm gives prime importance to achieve balancing of load in the network. The suitable energy node will be assigned as a forwarding node as long as this node has the capacity to handle. In this way a multi hop minimal less distant path is established to bounds the network damage from source routing attacks.

In our protocol avoids the collapsing of entire network by dropping the packets in the network. The load is evenly balanced depending upon the capacity of the nodes. In this way multi hop load balanced network is achieved.

Communication Phase

The main role of communication phase is to avoid the same data packets transmitting through the same node repeatedly to deplete the batteries fastly and leads to network death because of source routing attacks. The process of repeating the packets is eliminated by aggregating the data transmitting within the forwarding node and route the remaining packets safely to the destination. The data aggregation is achieved by first copying the content of the packet that is transmitting through the node. That copied content compares with the data packet that is transmitting through the node if the transmitted packet is same the node stops the data packet transmitting through the same node again and protect the depletion of batteries fastly. Then send the required data packets through the established node safely to the destination.

4.1. Average Energy Consumption for varying packet lengths

Fig 2 shows that the average energy consumption of the network with variable packet size. In this, data communication phase transmitting the size at varying packet lengths of 8kb/ packet and 10kb/per packet respectively. From the graph it is observed that when message length is 8kb/packet the energy is less than 1J and the energy consumption is greater that 1J when packet size is 10kb/packet. That is when the packet length is increased the average energy consumption of the network is more.

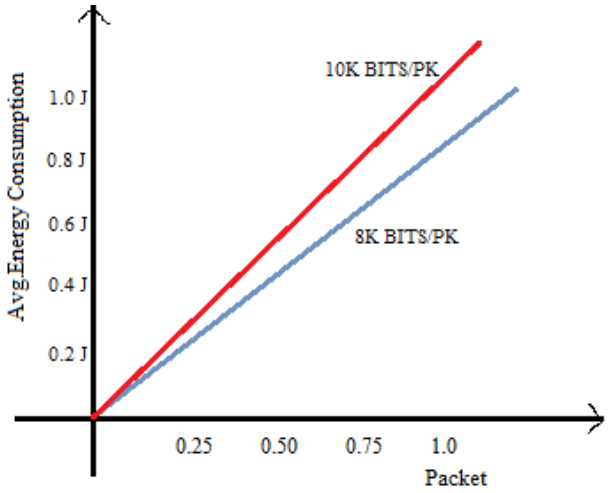


Figure 2: Average Energy Consumption for varying packet lengths

This is quite obvious because of greater overhead involved in aggregating the transmitting a larger sized packet. A packet length of 8kb/packet as lesser length packet may not in a position to carry out the desired task and a larger length may unnecessary contribute to addition overhead which can degrade the performance of the network.

4.2. Individual Energy Consumption

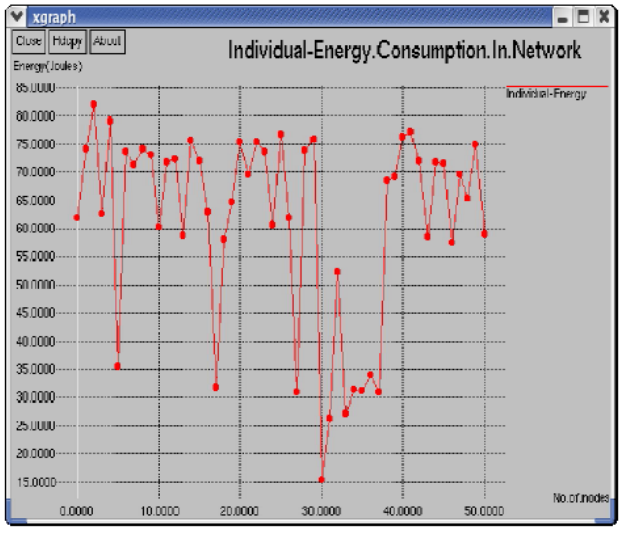


Figure 3: Individual Energy Consumption

Fig 3 shows that the individual energy consumption in the network that is the energy consumption of each node is shown in the analysis graph. Totally it is a network of 50 nodes. In the observation it is clear that energy consumption of every node is different. Initially all nodes have the initial energy of the 30th node is very low that is 15J and it is a compromised node.

Licensed Under Creative Commons Attribution CC BY

4.3. Average Path Length comparison

Fig 3 shows that the average path length comparisons of Energy Consumption in path length with compromised node path length. In the figure from the observation it is clear that compromised path length takes a hop count of approximately 150 but with ECMA it takes only a hop count of 60 for a network size of 50 nodes that is a compromised path takes 150 hopes for a message to reach its destination but with ECMA we can transfer with 60 hops to reach the destination.

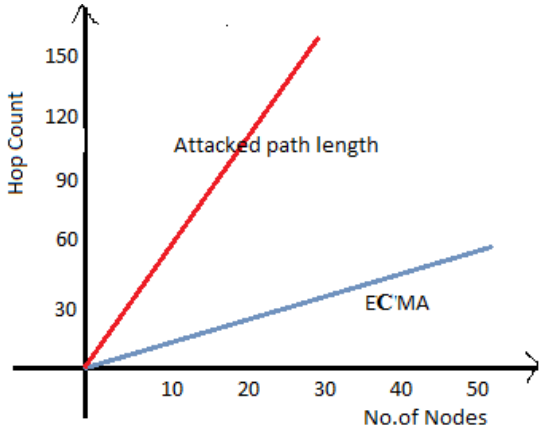


Figure 4: Average Path Length Comparison

From the analysis, we can easily understand how much energy is consumed to transfer a packet with 150 hops and with 60 hops. The 150 hops take more energy and delay than the packet travels with 60 hops is showed in fig 4. In fig 5 it clearly shows that the effects of the compromise node on the normal nodes. The analysis shows that if a node is compromised it will cause to death of nodes that is the nodes alive are rapidly decreased. As increase in the number of malicious nodes there is increase in the death of normal nodes.

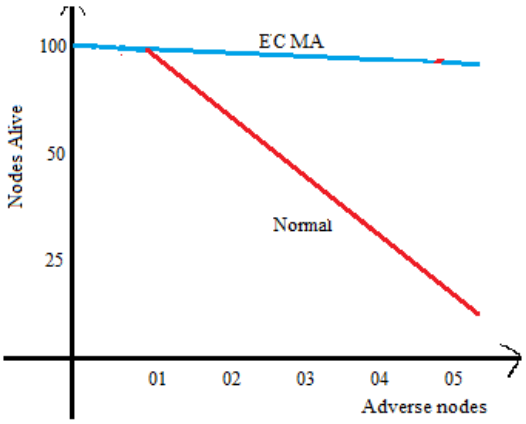


Figure 5: Effect of Vulnerable Nodes on the overall network

But with the ECMA we can increase the rate of nodes alive. It is clearly understand that if 5 nodes are affected with the vulnerable nodes it will approximately cause to death of 75 percent of nodes. ECMA concept greatly avoids the death of normal nodes only there are two or three nodes for the overall sensor network. Thus ECMA concept increases overall lifespan of network by energy efficient routing paths.

5. Conclusion

In this paper, we defined new class or resource consumption attacks that use routing protocols to permanently disable Adhoc wireless sensor networks by depleting nodes battery power. By the analysis overall performance of ECMA the results can vary according to the parameters. In this we have considered fixed number of nodes other parameters like energy can also be calculated. From this we can infer that routing protocols is necessary for better performance. Derivation of damage bounds and defenses for topology discovery, as well as handling mobile networks, is left for future work. Securing Adhoc networks is still an open issue. This paper will hopefully motivate future researchers to come up with smarter security and make network safer.

Acknowledgement

Most of all, I shall give glory, honor and thank to my family for their pray. I am very pleased of Professor Mr. B B K PRASAD, who spread no effort to ensure that I have everything I needed. Finally, thanks to the anonymous reviewers for their helpful comments on the earlier versions of this paper.

References

[1] Vern Paxson, An analysis of using reflectors for distributed denial-of service attacks, SIGCOMM comput. Commun Rev. 31(2001), no.3.
[2] Bryan parno, Mark Luk, Evan Gaustad, and Adrian Perrig, secure sensor network routing: A Clean-slate Approach, CoNEXT, 2006
[3] Haowen Chan and Adrian Perrig, security and privacy in sensor networks, computer 36 (2003), no.10.
[4] Srihari Babu. Kolla, “Defending against Source Routing Attacks and Packet Forwarding in Adhoc networks” in IJCSE volume 2, issue 4 Page no. 129-133. May 2014

Author Profiles



Mr. Srihari Babu. Kolla is pursuing Masters’ Degree in Department of Computer Science & engineering in Dhanekula Institute of Engineering & technology at Vijayawada in India. His research interests include Adhoc network, wireless networks and distributed systems.



Mr. B B K Prasad is an Associate Professor in Department of Computer Science & Engineering in Dhanekula Institute of Engineering & technology at Vijayawada in India. He obtained his Masters Degree in Computer Science from RAJAN engineering college. His research interests include Security for Sensor nodes and mobile applications, Computer Architecture, Networks on chip.

Licensed Under Creative Commons Attribution CC BY