A Survey on Detection and Prevention of Gray Hole Attack by Using Reputation System in Medical WSNs

DHANASHREE SUNIL GODSE[1], GANESH.R.PATHAK[2]
[1]*M.E Student, Department of Information Technology,*
Sinhgad College of Engineering, Pune, Savitribai Phule Pune University.
[2]*Professor, Department of Information Technology,*
Sinhgad College of Engineering, Pune, Savitribai Phule Pune University.

Abstract- A mobile ad hoc network (Medical WSN) is a persistently self-arranging, infrastructure-less network of mobile devices connected remotely. Each device in a Medical WSN is allowed to move independently in any path, and will therefore change its links to other devices frequently. Each must forward traffic irrelevant to its own utilization, and therefore be a router. The essential test in building a Medical WSN is preparing every device to continuously maintain the information required to appropriately route traffic. While mobile ad hoc networks have become a mature globally adopted technology due to its wide range of applications. Such environment has some basic differences in comparison to wired networks. Due to these little differences the Medical WSN are more prone to interception and manipulation. This further opens possibilities of insecure routing. For the efficient and secure delivery of data CRCMD&R (Cluster and Reputation based cooperative malicious node Detection and Removal) scheme is proposed in this paper. CRCMD&R suggests organizing the Medical WSN into a number of clusters and each node in the network has a specific prime number which acts as Node Identity. CRCMD&R uses Legitimacy value table and Reputation level table maintained by each node in the network to find and use a safe route between a source and a destination. The cornerstones of our work are the various metrics which can be further calculated by the values collected in Legitimacy value table and Reputation level table. Depending upon these metrics the cluster head nodes exclude or include the nodes from the discovered route and select the most reliable route to a specific destination. Contribution work is sending message in encrypted format for data security.

Keywords- Mobile Ad-Hoc Networks, Black Hole, Gray Hole Attack, Warm-Hole Attack, Denial-of-Service, Prime Number, Cluster, Security, Routing, Wireless Network, Packet Drop

I. INTRODUCTION

Wireless sensor networks (WSN), are similar to wireless ad hoc networks in the sense that they rely on wireless connectivity and spontaneous formation of networks so that sensor data can be transported wirelessly. Sometimes they are called dust networks, referring to minute sensors as small as dust. Dust Networks Inc. is one of the early companies that produced wireless sensor network products. WSNs are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to other locations. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring.

Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss is typically caused by network congestion. Packet loss is measured as a percentage of packets lost with respect to packets sent.

The Transmission Control Protocol (TCP) detects packet loss and performs re-transmissions to ensure reliable messaging. Packet loss in a TCP connection is also used to avoid congestion and thus produces an intentionally reduced throughput for the connection. In streaming media and online game applications, packet loss can affect the user experience.

Mobile Ad hoc Networks (MANETs) comprised of autonomous and self-organizing mobile computing devices which do not have a fixed infrastructure but rather they use adhoc routing protocols for data transmission and reception.

Ad hoc on demand distance vector (AODV) is an IP reactive routing protocol which is optimized for MANETs and it can also be used for other wireless ad-hoc networks. Nodes in network cannot perform route discovery or maintenance functions itself. This problem is resolved by using AODV as it computes the routing distance from sending node to receiving node at preset intervals.

II. LITERATURE SURVEY

Hindrance and Riddance of Gray Hole Attack In MANETs Multipath Approach, The paper [1] proposes a packet update scheme and even advise the elimination scheme by discovering all the malicious nodes. The overall simulation

performances is demonstrate that the Gray Hole attack scenario provides good result and even normalize the Gray Hole effect network which results in normalizing effects, of Gray Hole. Concept has shown improved result after elimination of the Gray Hole attack in the simulation result. Advantages are: Gray Hole attack scenario provides good result and even normalize the Gray Hole effect. Disadvantages are: To find out the entire malicious node, repeat the whole process which can take more time and resources too. It does not summarize attack contents.

An Approach to Prevent Gray-hole Attacks on Mobile ad-hoc Networks, The paper [2] proposed to detect and prevent gray-hole attack using multipath solution. Proposed technique based on alarm and alternate neighbor route mechanism. This is capable of detecting & preventing the single & cooperative malicious gray-hole nodes. To communicate via network path. This work considers gray-hole attack as study target and derives mechanism to spot and stop MANETs from security threat. Advantages are: Reduce the overhead of network and improved the network performance. Disadvantages are: The sub-event content and topic analysis, such that multiple views or temporal variations not represent in the nodes.

CRCMD&R: Cluster and Reputation based Cooperative Malicious Node Detection & Removal Scheme in MANETs, The paper [3] proposes CRCMD&R scheme suggests organizing the MANET into a number of clusters and each node in the network has a specific prime number which acts as Node Identity. CRCMD&R uses Legitimacy value table and Reputation level table maintained by each node in the network to find and use a safe route between a source and a destination. The open nature and low cost of implementation of wireless ad-hoc network make them prone to various security attacks. In communication frequencies 30MHz-5GHz large area in use for example vehicular ad-hoc network, smart phone in communication, internet, military in secure security system. Disadvantages are: Connection between nodes that communicate with each other. MANET is having Open nature that makes it vulnerable for various security threats. These vulnerabilities allow the attacker to compromise the network and degrade the performance of the network. The complete study concludes that a practical implementation is not a feasible solution.

Network-Layer Security in Mobile Ad Hoc Networks, This paper [4] describes the unified network-layer security solution in ad hoc networks, which protects both routing and packet forwarding functionalities in the context of the AODV protocol. The advantages of leveraging existing IDS matching technologies. Implementation directly using Network Layer Protocol. Disadvantages are: Insecure routing protocol and does not incorporate any mechanism to detect and prevent communication from malicious affect.

A Comparative Review on Routing Protocols in MANET, In [5] paper, the comparative study of DSDV, AODV, DSR, TORA, OLSR, WRP, DSDV routing protocols. These protocols can be divided into three classes‟ proactive class, reactive class and hybrid class. This classification of routing protocols is work according to their technique such as hop count, link state and QoS in route discovery. Disadvantages are: A single routing protocol can't perform best in all situations.

III. PROPOSED SYSTEM APPROACH

Ad-hoc On-demand Distance Vector (AODV) is one of routing protocols in Medical WSN that considered it in this study. It is a reactive routing protocol and creates routes from source to destination at the start of communication. In AODV protocol [5], source broadcasts RREQ packet to its neighbors to discover route to its destination. After gathering RREP packets from the neighbors, source selects the best route to its destination and sends data packets through that route. Black hole attack and gray-hole attack are two kinds of different possible attacks. In black hole attack, attacker replies to each RREQ packet of route discovery with the greatest sequence number that it can. Then source node selects the greatest RREP sequence number and also selects the route contained in that RREP packet. Attacker tries to spoof ID of destination node and by using a high sequence number in RREP flows all data packets to itself. Gray hole attack is a kind of black hole attack, in which one node occasionally drops packets of a destination. This node sometimes acts like a normal node and sometimes as not normal. Distinguishing of this attack is really harder than black hole attack because of frequently acting normal and frequently malicious.

This project makes three primary contributions:

- First, evaluate the vulnerabilities of existing protocols to routing layer battery depletion attacks.
- Second, shows simulation results quantifying the performance of several representative protocols in the presence of a single Gray Hole (insider adveECCry).
- Third, modifies an existing sensor network routing protocol to provably bind the damage from Gray Hole attacks during packet forwarding.

Advantages:

- The ratio of network-wide power utilization with malicious nodes present to energy usage with only honest nodes when the number and size of packets sent remains constant. Safety from Gray Hole attacks implies that this ratio is 1.
- An adveECCry constructs artificially long routes, potentially traversing every node in the network.

- Increases packet path lengths, causing packets to be processed by a number of nodes that is independent of hop count along the shortest path between the adveECCry and packet destination.

IV. SYSTEM ARCHITECTURE

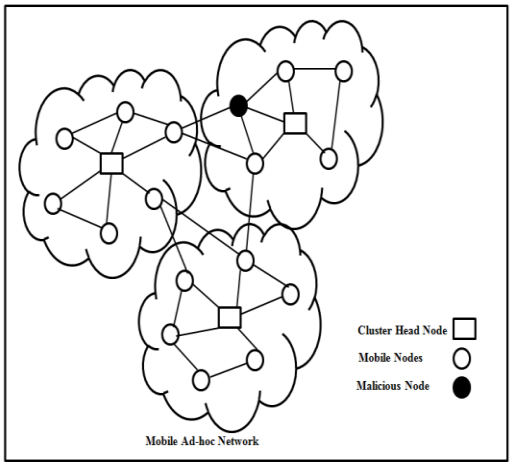

Fig.1 Proposed Architecture

Algorithm for Gray Hole Attack **Attack**

```
GH_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)
    }
    }
```

Algorithm for Carousel Attack Prevention

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

ECC Algorithm

Input: message, secret_key

Output: recover_message

Process:

1. Begin
2. Represent the message as an integer between 0 and (*n*-1). Large messages can be broken up into a number of blocks. Each block would then be represented by an integer in the same range.
3. Encrypt the message by raising it to the *e*th power modulo *n*. The result is a ciphertext message C.
4. To decrypt ciphertext message C, raise it to another power *d* modulo *n*
5. End

V. CONCLUSION

In this simulation, we send data in encrypted format for data security. The secure packet forwarding phase of clean slate routing protocol and prevent packets from Gray Hole attacks. But we have not secured discovery phase. In future by using synchronous discovery and ignoring discovery messages during intervening period. We can secure and damage limitations, and defense discovery phase. We study shortly some Gray Hole attacks, how they occurs in Clean Slate routing protocol (PLGP), how it can be avoided, detected in Clean Slate routing protocol with attestation (PlGPa), lastly we compare three protocols in some performance metrics. In the view of energy consumption better protocol is PLGPa as it prevent packet from circulating in loop. As in another metrics PLGP looks better due to some increased processing. PLGPa has little drawbacks but they can be avoided.

VI. REFERENCES

[1] Author-Dinesh Goyal, Savita Shiwani, “Hindrance and Riddance of Gray Hole Attack In MANETs Multipath Approach”, Published in IEEE in Feb, 2017.

[2] Author-Kusumlata Sachan, Manisha Lokhand, "An Approach to Prevent Gray-hole Attacks on Mobile ad-hoc Networks" Published in IEEE in Nov, 2016.
[3] Author- Saurabh Sharma, Sapna Gambhir, "CRCMD&R Cluster and Reputation based Cooperative Malicious Node Detection Removal Scheme in MANETs", Published in IEEE in Feb, 2017.
[4] Author-Hao Yang, J. Shu, "Network-layer security in mobile ad hoc networks IEEE Journal on Selected Areas in Communications", Published in IEEE in Feb, 2006.
[5] Author- Deepali A. lokare, Tarun Sharma, Aditi Kalia, "A Comparative Review on Routing Protocols in MANET", in International Journal of Computer Applications (IJCA) Vol.1, No.1, Jan 2016.