International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

A Method of Implementing Security in Multihop Wireless Systems

Poli Hari Krishna & Billu Mathan Baba
*Rollno: 1115112, Sree Vidyanikethan Institute of Management
**Assistant Professor, Sree Vidyanikethan Institute of Management

ABSTRACT:*Multihop remote systems are the kind of systems which require at least two remote bounces to convey the data from the source to goal. Along these lines finding an ideal and most secure way to course the information is the significant test. There are different steering conventions proposed for Multihop remote systems however the greater part of them are either unreliable or casual technique for thinking is utilized to investigate their security.In this paper, we intend to distinguish the safety efforts that could build the security of directing protocol.*

KEYWORDS- Routing, Routing protocols, Adversary, Security attacks, Authentication, Node disjoint paths.

I.INTRODUCTION

Routing is the strategy used to move an information bundle from the sender to collector. It empowers the messages to go from one hub (PC) to another driving it to at last achieve the goal. Each datum bundle contains inside it the arrangement of data including what is it, where it is originating from (sender's IP address) and where it is going (beneficiary's IP address). The gadget called as switch is utilized to perform steering in a system. While we consider steering in Multihop remote systems, it turns out to be tremendously important to locate the ideal and most secure directing conventions out of the current ones. The point of our examination is to secure these multihop remote system conventions. We have attempted to first talk about the different steering conventions and different security assaults on these directing conventions. At that point in the wake of talking about assaults on steering conventions, we have distinguished the safety efforts that could expand the dependability of the protocols.

II.LITERATURE REVIEW.

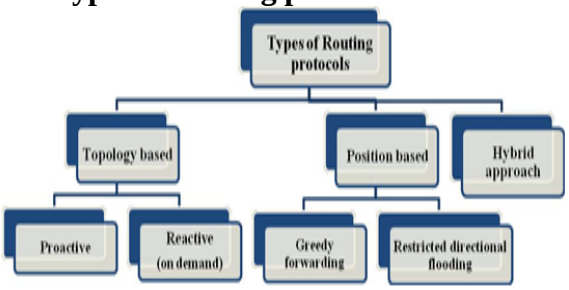
There are various numbers of researchers who proposed several architectures and protocols to secure the Multihop wireless networks.Srdjan Capkun, Levente Buttyan and Jean Pierre Hubaux [1] successfully presented SECTOR which is the mechanism to prevent the wormhole attacks and thus to secure routing protocol. SECTOR was based on distance bounding technique, on one-way hash claims and on Merkle hash trees.A new protocol called as BSMR was proposed by Reza Curtmola and Cristina Nita-Rotaru [2] that can withstand insider attacks from colluding adversaries.Douglas, Daniel, Benjamin and Robert [3] concluded in their work that the shortest path algorithm id not enough to increase the performance of multihop wireless networks.Jorjeta G. Jetcheva and David B. Joshnson [4] presented the informal design and they evaluated ADMR protocol.Yauchao Zhang and Yuguang Fang [5] successfully addressed the multihop wireless mesh network security. They also proposed ARSA which is an attack resilient security architecture for multihop wireless mesh networks.

III.ROUTING PROTOCOLS FOR MULTIHOP WIRELESS NETWORKS.

In order to enable the communication between the routers, routing protocols disseminates information about selecting routes between nodes in a network.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

3.1 Types of routing protocols.



"Figure 1. Types of Routing Protocols"

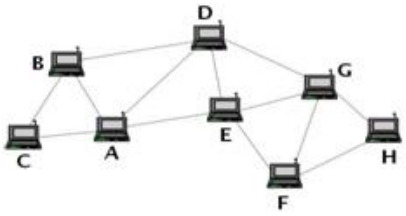
3.1.1 Dynamic Source Routing.

DSR protocol [6] is a type of on-demand routing protocol which is designed for use in multihop wireless network. it is self configuring protocol which eliminates the need for an established network infrastructure.

DSR follows two main mechanisms:

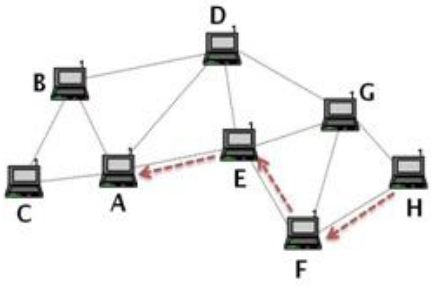
- Route discovery
- Route maintenance

These mechanisms work together to discover and maintain routes in a wireless network. When the ROUTE REQUEST reaches the destination node, the ROUTE REPLY message is generated. The destination requires a route or the route record in the ROUTE REQUEST message header.Route maintenance phase is initiated whereby the route error packets are generated at a node. Then the erroneous hop is removed from the node's route cache. All routes that contain the erroneous hop are truncated and again route discovery phase is initiated.



A → *: [RREQ, id, A, H; ()]
B → *: [RREQ, id, A, H; (B)]
C → *: [RREQ, id, A, H; (C)]
D → *: [RREQ, id, A, H; (D)]
E → *: [RREQ, id, A, H; (E)]
F → *: [RREQ, id, A, H; (E, F)]
G → *: [RREQ, id, A, H; (D,G)]

"Figure 2. Foot note: DSR route discovery"



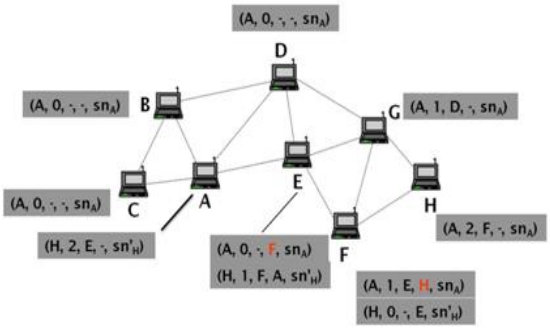
H ⟶ A:[RREP, <source route>;(E,F)]
Where;
<source route> is obtained:
• from the route cache of H
• by reversing the route received in the RREQ
• by executing route discovery from H to A

"Figure 3. Foot note: DSR Route Reply path"

3.1.2 Adhoc On-Demand Distance Vector Routing Protocol.

AODV is a reactive routing protocol which is capable of both unicast and multicast routing.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018



A → *: [RREQ, id, A, H, 0, sn_A, sn_H]
B → *: [RREQ, id, A, H, 1, sn_A, sn_H]
C → *: [RREQ, id, A, H, 1, sn_A, sn_H]
D → *: [RREQ, id, A, H, 1, sn_A, sn_H]
E → *: [RREQ, id, A, H, 1, sn_A, sn_H]
F → *: [RREQ, id, A, H, 2, sn_A, sn_H]
G → *: [RREQ, id, A, H, 2, sn_A, sn_H]

"Figure 4. Foot note: AODV route discovery"

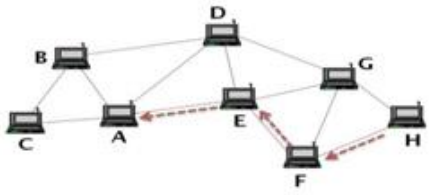
• When source sends data to an unknown destination it broadcasts a Route Request (RREQ) for that destination.
• When intermediate nodes receive Route Request (RREQ) a route to the source node is created.

• When RREQ reaches the destination node it generates a Route Reply (RREP) in a unicast hop by hop mode.

• Each intermediate node creates a route from destination to source during the propagation of RREP.

• Finally when RREP reaches the source, it tracks the route from destination to source and begin sending the data.

• The operation is similar to that of DSR but the nodes maintain routing tables instead of route caches.



H → F: [RREP, A, H, 0, sn'_H]
F → E: [RREP, A, H, 1, sn'_H]
E → A: [RREP, A, H, 2, sn'_H]

"Figure 5. Foot note: AODV Route Reply Path"

3.1.3 Position based Greedy Forwarding.

Position based routing or geographic routing [7] is a type of routing protocol that is based on the information regarding the geographical position. Mainly proposed for wireless network is based on the assumption that:
• Nodes are unaware of their own and their neighbor's position.
• The information about the position of the destination node is contained in the packet header.

In position based greedy forwarding protocol the packet is forwarded to the neighbor who is closer to the destination than the forwarding node.

IV. ATTACKS ON MULTIHOP WIRELESS NETWORKS.

The multihop wireless networks are wireless are widely accepted and its applications are increasing day by day. But the security of these networks is becoming a major key challenge in the wide-scale deployment of these networks.In simple and general context, an adversary is one's opponent in a contest, conflict or dispute.In the term of wireless network, an adversary is a node that opposes or attacks the security of the network and leading to an insecure communication in the network.These security attacks aim to increase the control of these adversary nodes over the

communication between some nodes in the network. These attacks tend to degrade the quality of the network services and also increase the resource consumption.Adversaries are not physically present but aim to corrupt the legitimate nodes by launching attacks from regular devices.

3.2 Types of Attacks.

The various types of security attacks are listed below:

- Route disruption
- Route diversion
- Creation of incorrect routing state
- Generation of extra control traffic
- Creation of a gray hole

3.2.1 Route Disruption.

In the route disruption attack the adversary prevents a route from being discovered between two connected nodes. The main objective of this attack is to degrade the quality of network services. The two connected nodes cannot communicate directly and therefore a route is followed that has the adversarial control. The attack mechanisms are:

- Dropping of Route Request or Route Reply messages
- Forging route error messages
- The dropping of control packet
- Wormhole attack

3.2.2 Route Diversion.

Route diversion attack leads to the establishment of the routes which are different from the ones that the protocol would establish due to the interference of the adversary. The adversary aims to achieve that the diverted routes should have its control over the link so that it can eavesdrop or modify the data that is been sent between the victim nodes.

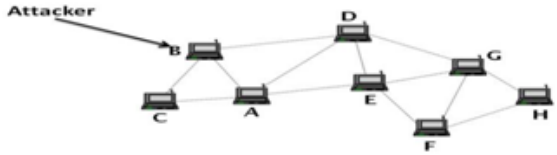
It also has side effects of increase in resource consumption, overloading the network links and delay in the delivery of the data.

The attack mechanisms are:

- Modifying or dropping control messages
- Setting up a wormhole/tunnel

3.2.3 Creation of incorrect routing states.

In this attack, the insecure and adversary nodes are appeared to be secure and the state appears to be correct but in fact they are not. So when the data packets are routed using the infected state they never reach their desired destination because of these corrupted nodes. This can be achieved by modifying, spoofing, forging or dropping of control packets.



"Figure 6. Creation of incorrect routing state in DSR"

The route specified by protocol is:

A = *: [RREQ, id, A, H ;()]

From the figure it is been clear that the route (A, D, F, H) does not exist.

Node B being an attacker creates an incorrect route:

B → A: [RREP, <src route>, A, H; (D, F)]

3.2.4 Generation of extra control traffic.

This attacks aims at injecting spoofed control packets into the networks. Spoofing is the technique of masquerading others by modifying or falsifying data resulting in gaining illegitimate advantage.

It leads to the increase in consumption of resources by flooding the illegitimate control packets in network.

3.2.5 Setting Up a Gray Hole.

Gray hole [9] attacks the network by leading the nodes to drop the packets selectively. This attack leads to the data to

be either malicious or unnecessary by dropping all UDP packets while forwarding TCP packet or by dropping packets by probabilistic distribution. Gray hole is actually an attacker node but behaves as a correct one. Therefore, it becomes very difficult to identify the attacker node in the network.

V.SECURING MULTIHOP WIRELESS NETWORK ROUTING PROTOCOL.

After discussing several attacks that could degrade the quality of the network, we aim to list out various security countermeasures that could help to increase the security and prevent these attacks.

4.1 Countermeasures.

- Authenticating control packets
- protection of mutable information in control packets
- Reducing gray holes from the network

4.2.1Authentication of control packets.

In the network whenever a packet is transmitted it has two sets of information: control information and user data often called as payload. the control information contains the source and destination addresses, checksums and sequence information. The adversaries often attack the control information of the packet in order to degrade the quality of service. Control packets should be authenticated by the initiators of the packet using Message Authentication Code and the authenticity should be verifiable by the destination node.For example Ariadne which is used to secure the basic version of DSR algorithm.Now when this packet reaches any intermediate node, that node must be able to verify its authenticity before processing the control packet. After the verification, the intermediate nodes update their routing state. A Broadcast Authentication scheme must be employed to verify the authenticity of the nodes.

4.2.2Protection of Mutable Information in Control Packets.

There are certain set of inconstant information that can be altered or changed throughout the network. This mutable information (hop count, node list etc) is added by intermediate nodes to the control packets before forwarding it. Since this information is not protected, the adversary could easily attack and modify making it malicious.To prevent this, each intermediate node before entering or modifying this mutable information should verify its authenticity. If the node is found authenticated to enter or modify the information then only it is liable to alter any information.

4.2.3Combating Gray Holes

Gray holes are very difficult to detect in a network. It is much easier to deal with an attacker rather than detecting it out of the correct nodes. In order to reduce these gray holes, multiple routes should be traced out to deliver a data packet. It would be preferable if these routes are Node Disjoint paths [10]Node Disjoint Paths reduces routing overhead and also provides robustness to mobility. To decrease the resource consumption, the data packet should be coded and then break up into smaller chunks. If a threshold value is set for the number of chunks then it will prove beneficial to the network. Then these chunks of packet are sent over different routes on entire network.

CONCLUSION.

As we all are aware that in Multihop wireless networks several intermediate nodes are present which are also movable. So routing is a major challenge in these networks as it becomes immensely necessary to save the nodes from the attacks. In this paper, we have discussed various routing protocols and a brief

description of various attacks is also given which can harm the Multihop wireless networks. After discussing these attacks we have finally discussed several countermeasures that could help to secure the routing protocols from the adversarial attacks by the authentication.

REFERENCES.

[1.]http://www.enggjournals.com/ijcse/doc/IJCSE10-02-03-04.pdf
[2.]http://dl.acm.org/citation.cfm?id=986862
[3.]http://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=2669&context=cstech&sei-redir=1&referer=http%3A%2F%2Fscholar.google.co.in%2Fscholar%3Fq%3Dbsmr%26btnG%3D%26hl%3Den%26as_sdt%3D0%252C5%26as_vis%3D1#search=%22bsmr%22
[4.]http://am.csail.mit.edu/papers/grid:hotnets02/paper.pdf
[5.]http://www.cs.rice.edu/~dbj/pubs/mobihoc01-admr.pdfs
[6.] http://nslab.kaist.ac.kr/courses/2007/cs712/security%20misc/1.%20ZHA06%20(ARSA%20-%20An%20Attack-Resilient%20Security%20Architecture%20for%20Multihop%20Wireless%20Mesh%20Networks).pdf

[7.]http://en.wikipedia.org/wiki/Dynamic_Source_Routing
[8.]http://en.wikipedia.org/wiki/Geographic_routing
[9.]http://www.ijcnwc.org/papers/vol2no62012/2vol2no6.pdf
[10.]http://140.116.247.229/member/Marco/data/On-demand%20Node-Disjoint%20Multipath%20Routing%20in%20Wireless%20Ad%20hoc%20Networks2.pdf