Research Paper
Impact Factor - 2.262
Peer Reviewed Journal

IJMDRR
E- ISSN –2395-1885
ISSN -2395-1877

SECURITY IN WANET USING ADMIN SELECTIONALGORITHM

K.Krishna Veni B.Tech (IT) * **T.Rajadurai M.Sc (CS & IT) ***
**Department of Computer Science Saiva Bhanu Kshatriya College, Aruppukottai, Tamil Nadu.*

Abstract
In this paper we discuss about how to make a secure connection in Wireless Ad hoc Network (WANET). In WANET a malicious device may be present. It can attack the devices in network by spoofing. To identify the malicious device, we can set a device in WANET as admin in each region. When a device enters in a region it must be registered with the admin. After registration only the device can communicate with other devices within its range. If the device wants to send the data to a device out of its range, it can communicate via admin only. In this process the malicious device cannot access the data. It also reduces the number of Redundant Data Forwarding, as it forwards the data to only admin and destination. The selection of admin device is a very important process. The changes in admin's status and any device must be updated. In this process before sending the data using reactive routing protocol type, the route for the destination via admin is determined and communication is processed.

Keywords: WANET, Admin, Spoofing, Registration, Routing.

I. INTRODUCTION

A Wireless Ad-Hoc Network (WANET) is a collection of wireless devices that can communicate with each other without any dependence on a fixed infrastructure or centralized administration. Devices within transmission range can communicate directly with each other, but those out of range must rely on other devices to forward along packets to their final destination [2]. Because they can be deployed quickly and require no extra planning, ad hoc networks are often useful for establishing temporary work- groups in war-room settings, single building business meetings, or disaster relief situations. But in this scenario security is a very important issue. When a malicious device comes into a range of a device in WANET, It can directly communicate with the devices in its range as an authorized device [3]. To overcome the security issue, I proposed an Admin Selection Algorithm. In this algorithm any authorized device in a WANET can be selected as Admin for every Hop Range. Every device in WANET must be registered with the admin in its range. So any malicious device cannot access the WANET directly.

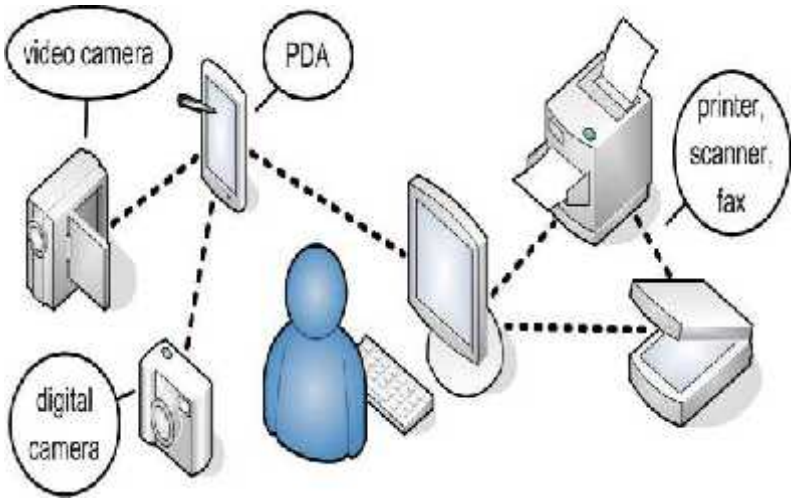

Figure: 1. Wireless Ad Hoc Network Environment

II. AD HOC NETWORKING

In ad hoc network devices within transmission range can communicate directly with each other, but those out of range must rely on other devices to forward along packets to their final destination [1].

IJMDRR
E- ISSN –2395-1885
ISSN -2395-1877

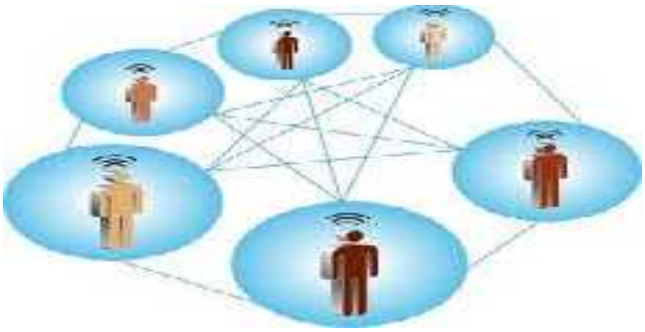

Figure: 2. Communication in Ad Hoc Network

Routing enables communication between devices that cannot communicate directly. In the ad-hoc network, using an ad-hoc routing protocol does this. There are two types of routing protocols for ad-hoc networks: Proactive and Reactive. In proactive routing, routes are actively maintained, and they are available when needed. In reactive routing, routes are discovered on demand [1].

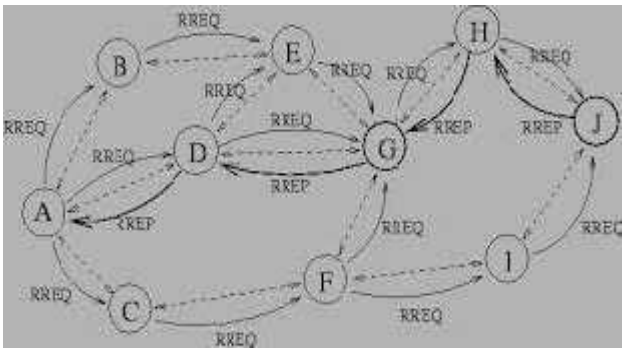

Figure: 3. Route Discover in Reactive Routing Protocol

III. SECURITY ISSUES IN AD HOC NETWORK Wireless networks are more vulnerable to misuse than wired networks. In a wireless network, all devices share the same radio band. A malicious device may be present in the network. It can analyse the communication in the network and do several attacks by sending invalid data [4]. It is impossible to prevent a malicious device from interfere the transmission in a wireless ad-hoc network. This issue can be overcome with the Admin Selection Algorithm and Registration process with the admin based on encrypted IP Address.

Figure: 4. Attack in Ad Hoc Network

Research Paper
Impact Factor - 2.262
Peer Reviewed Journal

IJMDRR
E- ISSN –2395-1885
ISSN -2395-1877

IV. ADMIN SELECTION ALGORITHM

1. In this algorithm any nodes in each Hop distance is selected as admin initially.
2. Every node within the range of admin node must be registered with admin.
3. For registration every node forwards request to all devices.
4. Only admin nodes will response with its encrypted IP address.
5. The authorized devices can only decrypt the
6. IP address.
7. Then the devices will register themselves to the admin properly.
8. The admin will maintain the details of all registered nodes and the details of nearest admin.
9. Only registered user can only communicate in WANET via Admin node.
10. If a device receives response from two or more admin, then the device will prefer to one of the nearest admins only.
11. Malicious devices cannot access the network without registration.
12. As the Encrypted IP address is used for registration, malicious device cannot register with the admin.
13. If a node wants to send the data to a node *within its range*, it can send the data directly to the node.
14. If a node wants to send the data to a node *out of its range*, it sends that data directly to its admin.
15. The admin then flooding the data to the nearest admins.
16. Every admin which receives the data will check whether the destination node is available in its range.

a. If so that admin will send the data to the destination node.
b. Otherwise it again forwards the data to the next admin.

A .Admin Selection & Registration

In admin selection algorithm initially during network creation the selection of admin node is very important. After network creation, for every hop distance a device is selected as admin. The device has a *register* to store the status of the device as *admin or Non Admin*. After the selection of admin, every device sends a request message to all devices in their range. For that message admin devices only will response with its encrypted IP address. The authorized device can only decrypt the IP address. The devices then send a registration request to the admin. After registration only all devices can send data to another device including admin device. So admin selection and registration is most important in this algorithm.

B. Route Management in Proposed System

In Ad hoc Network as the devices are in mobility, it is very difficult to maintain a stable network. When a device moves, the routes must be updated in Ad hoc Network [2]. In Admin Selection Algorithm the route management must be done by two strategies using AODV protocol. In one strategy the *route for admins* is managed and in another strategy the *route for other devices* which are not acted as admin. In admin's route management, if admin changes its position, the status of admin must be sent to all devices registered with the admin and to all the admin devices. Then the devices which are now out of region of the admin must be registered with other admin within its range and the details of the register in the previous admin node must be also updated. In device's route management, if any device changes its position, it must be updated to its admin. During movement of device if it moves out of the admin's region, the device must now register itself with a new admin in its range.

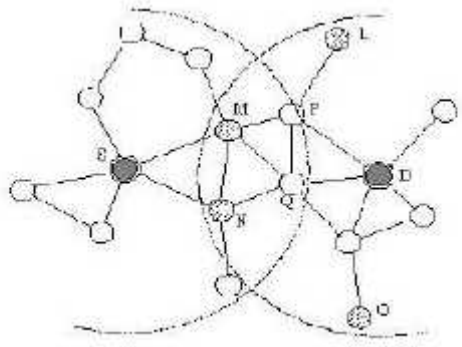

Figure: 5. Route Management in Ad Hoc Network

If it does not move out of the admin's range, the device simply needs to update its details to the admin. If in the same region two admins presents, the devices must choose the admin which are nearer to them.

C.Communication in Proposed System

When a device wants to send a data to another device in its region, it first request for route via admin device to all the devices within the admin's range. After route has discovered it maintains the route and start transmission of the data to the destination device via the route discovered. When a device founds that the destination device was out of its region, it simply forwards the data directly to its admin. After that the admin device will flood the data to all the admin devices. The admin node which does not have the destination device in its range will forward the message to other admins.

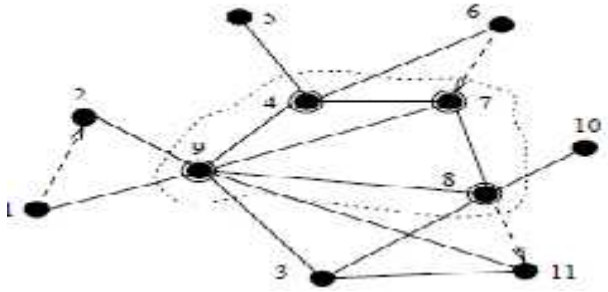

Figure: 6. Data Forwarding in Ad Hoc Network

The admin which has the destination device in its range will found the route to transmit the data. After receiving the data the destination device sends the acknowledgement with its admin details also. So the admin of the source node will directly sends the data to the admin of the destination node in further data transmission. If the destination node changes its position or its admin, the last admin of the destination node will forward the data to the destination via new route or to the new admin. Due to this admins play a vital role in transmitting data to a device which are out of the range of source node.

V. CONCLUSION

In this paper I have proposed an algorithm named *Admin Selection Algorithm* to ensure the security in transmitting the data in Wireless Ad hoc Network. As the all the nodes have to register with the admin node with the encrypted IP address, there is no possibility of malicious device to enter into the network. As the data which needs to be sent to the device out of the device's range is only forwarded to admin nodes only, there is no need of ending data to every intermediate node in the network. Due to this rate of ending redundant data is reduced.

VI. FUTURE WORK

In admin selection algorithm even though security is assured, the initial network setup is complicated. User always prefers quick network setup activities. So to improve the performance of the network, the initialization process must be simpler.

ACKNOWLEDGEMENT: We wish to acknowledge our colleagues Mrs. A. Jothi Priya, Asst., Professor in Maths (CA), Mr.S.Balamurugan, Head of the Department in CS and we would like to acknowledge our Principal Dr.N.Muthuselvan M.Com., M.Phil., Ph.D. for their technical & moral support to make this research. We also thank them for their whole hearted support.

REFERENCES

1. N. Sadagopan, F. Bai, B. Krishnamachari, and A. Helmy, 'Paths: analysis of path duration statistics and their impact on reactive manet routing protocols," in MobiHoc '03, 2003.
2. M. Gerharz, C. de Waal, M. Frank, and P. Martini, 'Link stability in mobile wireless ad hoc networks," in Proceedings of the 27th Annual IEEE Conference on Local Computer Networks (LCN'02), Tampa, FL, November 2002, pp. 30-39.
3. C. Perkins, E. Belding-Royer and S. Das, 'Ad hoc on-demand distance vector (aodv) routing," RFC 3561, 2003.
4. Virendra Pal Singh1, Sweta Jain and Jyoti Singhai, 'Hello Flood Attack and its Countermeasures in Wireless Sensor Networks', IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 11, May 2010.