ISSN: 2278-4632
Vol-11 Issue-02 2021

Secure Neighbor Discovery in Wireless Networks by Detecting Various Attacks

Sanjaya Kumar Sen[1], Bijay Kumar Gouda[2]
Department of CSE, EATM, Bhubaneswar

Abstract

Neighbor discovery is an essential part of many protocols for wireless networks which includes routing, leader election within a cluster and group management. If the detection of neighbor fails, communication and performance of the protocol decreases. Wireless networks as the name indicates uses the Radio Frequency (RF) as communication medium and are extensively being used in various military and commercial applications. Wireless networks, due to their nature of deployment are vulnerable to various attacks. Wormhole or Relay attack, Selective dropper attack, Cloning attack, Denial of Service (DoS) attack and Modifier attack etc. In this paper we present the Mobile agent based method which offers a measure of security against various attacks by allowing participating nodes to determine whether they are the neighbors.

Keywords*:* Mobile agent; Wormhole attack; DoS attack; Cloning attack; Wireless networks

I. INTRODUCTION

Wireless Networks constituting large number of nodes are becoming possible solution to many demanding domestic, military, and commercial applications. Wireless Networks collect and distribute data from the fields where common networks are unreachable for various strategic and environmental reasons. Neighbor discovery is an essential first step in the initialization of a wireless network, since information of one-hop neighbors is essential for medium access control protocols [1], routing protocols [2], [3], and topology control algorithms [4] to work efficiently and correctly.

Wireless networks do not have centralized administration and are decentralized peer to peer network with self-configurable and self-organizing capabilities. Due to unpredictable topology wireless networks are vulnerable to attacks which include security and routing. Neighbor discovery is the procedure by which a node in the network determines the identity and number of nodes within its coverage range. Wireless networks are liable to the following kinds of attacks.

Relay or Wormhole attack: In this type of attack two are more wormhole nodes are connected via low latency wormhole link. A node that captures data from the source and directly relay to other wormhole node and hence by making *false neighbors* to communicate.

Figure Fig.1 shows the scenario of wormhole attack [5] in wireless networks. It may be observed that the nodes are in the form of router because both the wireless nodes and router are having capability of storing and forwarding the packets. The Green router indicates the source and destination nodes, blue router indicate the intermediate nodes and the red router indicates wormhole nodes which are connected via wormhole link. If the data packet has to betransmitted from source to destination node it has to travel either by path of hop count 5 or hop count of 6 but with the presence of wormhole nodes packet, will take the path with the hop count 2 by making source and destination nodes as neighbors, where in practical they are not.

ISSN: 2278-4632
Vol-11 Issue-02 2021

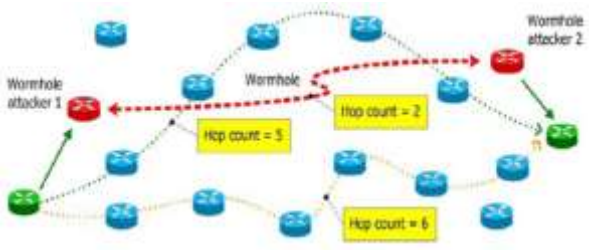


Fig.1: Wormhole Attack in wireless networks

Cloning Attack: Cloning attack is the entry point to a large span of dangerous attacks. In such attack, an opponent uses the credentials of a compromised node to surreptitiously introduce replicas of that node into the network. These replicas are then used to launch variety of attacks that subvert the goal of the wireless application, and the operation of the basic protocols. The detection of node duplication attacks in a wireless network is therefore a primary problem. A growing body of protocols has been proposed in recent years for detecting node replication attack in wireless networks. Most of them however expose the following limitations: performance outflow, difficult assumptions, necessity of inner control, lack of tidy attack detection etc.

Selective Dropper attack: One of the fundamental principles of wireless networks is that, it works on the concept of *"*Multi hop*"*. i.e. the wireless node that receives the message will forward it to the next node in that path. However, unluckily it is not the case in "Selective Dropping" attacks. In Selective Dropping the attacker attacks on one of the wireless nodes and infects it with a malicious code which in turn acts just like any other normal node in the wireless networks. Instead of forwarding the node in the path to next node, it just drops those data packets which make them act like a failed node [6]. Figure Fig.2 shows selective dropper attack. It is observed that while transmitting packet from source node to destination node the attacker node shown in orange colour will drop the packets instead of forwarding it to next node in network.

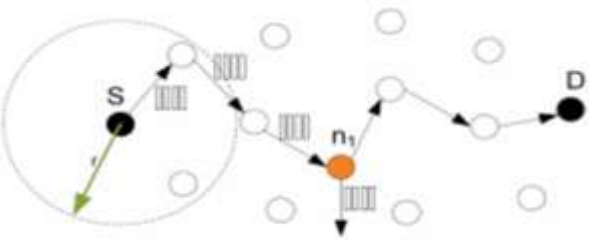
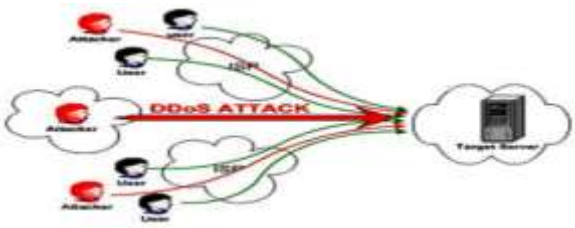


Fig.2 Selective Dropper attack

Denial of Service attack: Denial of service attack (DoS) [7] is an explicit attempt to prevent the legitimate user of a data. The general method of attack involves overfilling the target system with requests, such that it cannot respond to legal traffic. As a result, it makes the system unavailable for the user. The basic types of attack are: utilization of bandwidth or utilization of processor time, obstructing the communication among two machines, interruption of service to a specific system, etc.

Figure Fig.3 depicts the example of Dos attack. It is observed from figure that the attacker is flooding unnecessary request to the targeted server and making it unavailable to the legitimate traffic.



ISSN: 2278-4632
Vol-11 Issue-02 2021

Fig.3: DOS attack in wireless network

Modifier attack: It describes the threat that wireless data can be captured and modified during the process of transmission from one node to other.

The neighbor discovery algorithms have the following properties: 1) Do not require nodes to have *a priori* knowledge of the number of neighbors, 2) Do not require synchronization among nodes, 3) Allow nodes to begin execution at different time instants, and 4) Enable each node to detect when to terminate the neighbor discovery process.

The Rest of paper is prepared as follows: In section II we discuss some of the existing approaches which have been used to tackle the wormhole attack. Section III gives general idea of Mobile agent. Proposed solution is covered in section IV and Security and Simulation results shown in section V, followed by Conclusion in VI.

II. EXISTING APPROACHES

Several protocols have been proposed for finding the secure neighbor discovery by detecting the presence of various attacks. Many methods influence physical properties of communications which are explained as follows.

1) Location-based approaches

The location based approach [8] is divided into two categories they are.

(i) Geographical Leashes: Here the packet which is ready for transmission from one node to other is authenticated with time stamp and their location at the time of transmission with loosely synchronized clocks (with allowable margin) and on the receiver side the packet is examined whether it originates from sender which is within its communication range. This ensures physical neighbor discovery. In this approach each node need to be equipped with radio propagation model to determine the location is a communication neighbor. This requirement is impractical and hard to satisfy in communication environment which is highly dynamic.
(ii) Temporal leashes: When temporal leashes are used, the sending node append the time of transmission to each sent packet 'Ts' in a packet leash, and the receiving node makes use of its own receiving time 'Tr' for verification. The sending node calculates an expiration time 'Te' after which a packet should not be received, and put that information in the leash. Here in this approach the packet is attached with the expiration time and both sender and receiver are needed to be tightly synchronized. The drawback of this technique is timing synchronization which is subject to attack and wormhole can still change time of packet hence it does not provide physical neighbor discovery.

2) Directional antennas approach

Directional antenna [9] systems are increasingly being recognized as a powerful way for increasing capacity and connectivity of wireless networks. The use of directional antennas for relay attacks is proposed under the assumption of the unit disk model, the availability of antennas with an even number of non-overlapping zones identically oriented for all nodes. But this would ensure physical neighbor discovery against at most two external adversaries which are in opposite directions. In addition its applicability is limited as device in many mobile computing scenarios uses antennas which are only Omni-directional.

4) Connectivity Approach

In multi-hop networks, local network connectivity information is proposed as the basis of a heuristic to detect wormholes and reject false links and thus protect neighbor discovery against external adversaries. The strength of the connectivity approach is its practicality, in the sense that it does not require any specialized hardware or capabilities. Nodes exchange locally communication neighborhood information, obtained through a non-secure Neighbor Discovery mechanism. Afterwards they check for forbidden structures, i.e connectivity sub graphs that would exist if a wormhole were present. Forbidden structures depend on node density and the connectivity model. Unless the density is low, simulation results show a 100% detection rate with no fake alarms, for all connectivity models considered in. However, the simulations assume a relatively naive relay, whereas a selective wormhole establishing only one or few fake links would be less likely to create a forbidden structure.

3) Ranging approach

In ranging approach [10], ranging operation is considered that is the distance between two nodes over which packet

ISSN: 2278-4632
Vol-11 Issue-02 2021

can be sent. The wormhole is detected due to the fact that the path travelled by a ranging signal varies from expected value when a wormhole is present. If node A and B are correct neighbors then the ranging length would be R_i. If they are connected via wormholes than ranging length will be sum of two ranges.

Fig.4: Showing range between A and B; $R_i = R_1+R_2$

In Figure Fig.3 it may be observed that the Range perceived by the node A and B will be sum of two ranges of R_1 and R_2. This approach will work for small number of nodes and not feasible to larger networks.

4) Survey on cloning attack detection

Some of the existing algorithms [11] to detect Cloning attack of wireless network use centralized approach. Each node will send to a base station a list of its neighbors together with a location. The base station verifies that no node is in two (non-adjacent) locations at the same time. The central station receives and processes O(n) messages, but this is not generally an issue as it does not have the memory, communication and processing constraints of the nodes. This generates O(n) messages on the network and the node memory usage is null. The two main drawbacks of this approach is the existence of a single point of failure and, second one it need to have active base station. A third drawback is the large unbalance of message processing. Indeed as all the traffic goes to the same destination, nodes close to the base station will be quickly overwhelmed receiving and sending O(n) messages. On the other hand the nodes on the periphery will just send O(1) messages.

5) DoS detection method

DoS attacks are certainly not a new occurrence. The techniques used to cope up from common DoS techniques. Some of the types of DoS attacks are described below.

a) Consumption of limited or scares resources(network bandwidth, memory)
b) Alteration or destruction of configuration information.
c) Physical destruction of network components.

The devices which can partially or entirely disrupt the nodes signal by increasing the power spectral density are jammers. Parameters such as strength of signal, location and type of jammer have great influence on the performance of the network. One more physical layer attacks include node tampering. It is not very easy to totally prevent destruction of nodes; however masking and redundant nodes can mitigate this threat [12].

6) Selective Dropper & Modifier detection method

To deal with packet droppers, a widely adopted countermeasure is multi-path forwarding [13], in which each packet is forwarded along multiple redundant paths and hence packet dropping in some but not all of these paths can be tolerated. This scheme introduces high extra communication overhead. Another category of countermeasures is to monitor the behaviour of forwarding nodes. However, these schemes are subject to high energy cost incurred by the promiscuous operating mode of wireless interface.

To deal with packet modifiers, most of the existing techniques [14] are to filter the modified messages within a certain number of hops. However, without identifying packet droppers and modifiers, these countermeasures cannot fully solve the packet modification problems because the compromised nodes can continue attacking the network without being caught. To deal with packet modifiers, most of the existing countermeasures are to filter modified messages within certain number of hops. However, without identifying packet droppers and modifiers, these countermeasures cannot fully solve the packet modification problems because the compromised nodes can continue attacking the network without being caught.

III GENERAL IDEA OF MOBILE AGENT

Software agents capable with the property of mobility are called mobile agents. Mobile agents [15], [16] refer to programs that perform certain tasks on behalf of the user.

ISSN: 2278-4632
Vol-11 Issue-02 2021

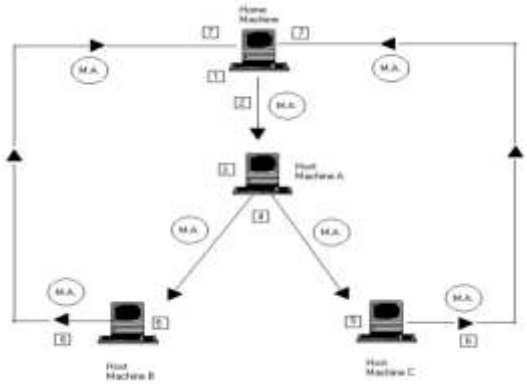


Fig.5: Mobile agent creation

The life cycle of mobile agent takes following steps:-

1. The mobile agent is *created* in the home machine.
2. The mobile agent is *dispatched* to the host machine A for execution.
3. The agent executes on host machine A.
4. After execution the agent is *cloned* to create two copies. One copy is dispatched to host machine B and the other is dispatched to host machine C.
5. The cloned copies execute on their respective hosts.
6. After execution, host machine B and C send the mobile agent received by them back to the home machine.
7. The home machine *retracts* the agents and the analysis of data which is brought by agents is done. The agents are then *disposed*.

Mobile agents comprise the following unique properties:

Autonomy: The mobile agent themselves decides sequence of operation to be performed and they do not involve any human interaction. They can take some decision by own for example they are free to choose node when to migrate to targeted node.

Adaptability: The mobile agent can learn from the experience and it has got a unique property of adaptability with the environment. They monitor traffic in large networks and detect the trouble spot within network.

Mobility: As name itself indicates mobile agents are capable of moving throughout network.

Mobile agent has the following advantages:

Decrease in network load: Mobile agents perform the computations at the remote hosts and return back with the results. Since computations are moved to the data storage location instead of moving data to the location where computing is done, hence load on network is reduced.

Asynchronous and Autonomous Execution: Mobile agents run asynchronously. Once a mobile agent is released from the home machine, the home machine can disconnect from the network. The mobile agent executes autonomously without the involvement of the home machine. The home machine can reconnect at a later time and collect the agent.

Remote filtering and searching: If everyone information was stored in structured databases, it would adequate to send a message to the server containing SQL statements and perhaps perform backend filtering on the results of search. Since most of the world's data is in fact in flat, free text files, remote filtering searching and does require the capability to open files, read, filter and possibly develop an index. Agent programs are certainly a probable method of performing this service

ISSN: 2278-4632
Vol-11 Issue-02 2021

IV. PROPOSED SOLUTION

In this paper we present the solution which is based on the Mobile agent concept which allows neighbors to make sure that they are communicating directly with each other.

We propose an algorithm that is based on Mobile agent traversal. The proposed solution is prepared to make communication between the correct neighbors by detecting the presence of attacker nodes.

d_{AB} – This function gives the distance between two neighboring nodes [for example A & B].
d_{AB} = (r-D) / v
Where r -Transmission range;
D- Distance between Node A and B.
v- Average speed of the node.

Network Model is taken as follows Let G = (V, E) represent a multi-hop wireless network, where V denotes the set of nodes and E denotes the set of directed edges in G. The definition of an edge is that an edge exists between nodes *i* and *j* if they are within the transmission range of each other and the edges between nodes are assumed as symmetric edges i.e if (i, j) □ E, then (j, i) □ E.. We assume that the nodes have *unique* identifiers i.e., no two neighbors of a given node have the similar identifier. The identifier possibly will be the MAC address of the node. And each node is equipped with a radio transceiver that allows a node to either transmit or receive messages, but not both simultaneously.

System architecture of proposed solution is given as follows

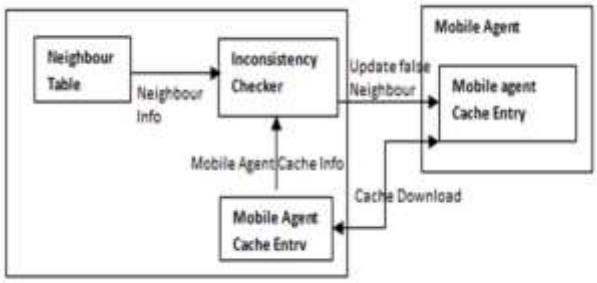


Fig 6: System Architecture of Mobile agent based solution

Mobile agent contains the some memory to store the neighborhood information and each wireless node also contains neighborhood table to store details about their neighbors. An Inconsistency checker is present to find out any uneven thing which happens when there is presence of relay attack. We using JProwler simulator is a distinct simulator which is running under MATLAB to demonstrate our proposed solution is having better results than previous methods.

Proposed Algorithm:

```
MobileAgent (int num,WirelessNetwork wn)
 {
nodes visited = new Boolean[num];
Wireless network  = wn;
 all claim = num
 }
 MobileNodeVisiting()
 {
 for (int i=0; i <all nodes length; i++)
```

{
MobileAgentVisiting = true;
}}

The Steps involved are as follows

1) Randomly Generate wireless nodes from 0 to maximum numbers with one or more Base Station for maintaining Mobile Agent.

2) Select the type of attacker from drop down menu like wormhole, selective dropper, cloning, Dos attacker etc.
3) After selecting particular kind of attack make Mobile Agent to traverse throughout the network.
Mobile agent randomly visits very node.

When mobile agent visits a node i,
- It checks the rate of receiving packets for that node to detect selective dropper attack.
- If it finds '0' (No packet from node j to node i) for neighboring node j,
- It doubts node j is a attacker node.
- It checks the location *claim mismatch* for detecting a clone attack.
- It checks the *checksum* violation for detecting modifier attack.
- While routing it checks for DoS attack for *flooding* unnecessary data.
- It detects presence of *wormhole* node and informs other nodes not to go through that node.

It starts routing process algorithm through multiple base stations for time t.
Within time t
It confirms whether node j is a attacker node or not.
If node j is an attacker node, it revokes node j.

4) After time t, it triggers routing process algorithm through nearest base station.(without using multiple base stations)
5) Mobile agent will Broadcast Packet which contains neighborhood information of every node in network and check for inconsistency.
6) Repeat step from 1 to 5 after every configurable time span until all attacker nodes are detected and make correct node to communicate.

V. SIMULATION AND RESULT ANALYSIS

Simulation Results:

The Proposed work was simulated using open source simulator called Jprowler. Prowler is a probabilistic simulator written in MATLAB and has a version in java (JProwler). The following graph results are obtained by considering different number of wireless nodes.

Simulator Parameters are as follows:

Parameter	Value
Network scale	200m x 200m
No. of wireless nodes	25~400
Mobile agent code size	500 bytes
Bytes accumulated by the mobile agent at each wireless node	100byte
Mobile agent execution time at each node	50ms

We obtain the following graphs with *multiple base stations with always* versus *multiple base stations during detection* of attacker nodes.

ISSN: 2278-4632
Vol-11 Issue-02 2021

Figure Fig.7 shows Graph of energy consumed versus number of nodes for existing approaches it is clearly observed that energy consumption is more with the multiple base stations present during detection of attacks.

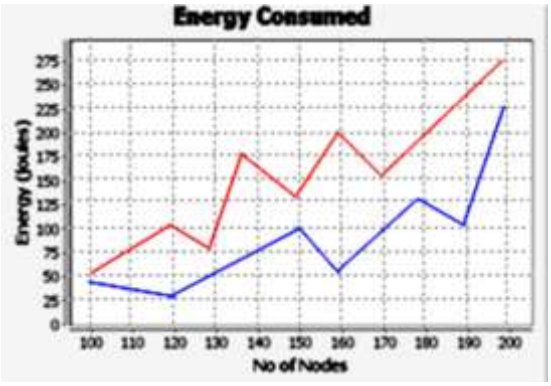


Fig.7: Energy vs No of nodes
Red line- Multiple base stations with always
Blue line- Multiple base stations during detection

Similarly Figure Fig.8 shows Graph of energy consumed versus number of nodes for our proposed solution it is clearly observed that energy consumption is less when compared existing methods

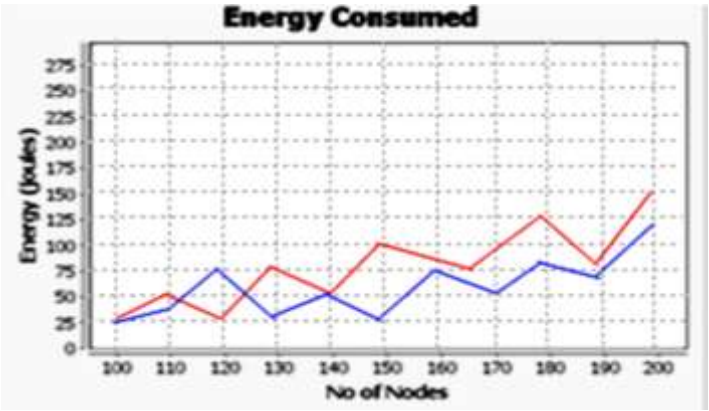


Fig.8: Energy vs No of nodes
Red line- Multiple base stations with always
Blue line- Multiple base stations during detection

The results shows that when number of wireless nodes are more for example 200 nodes the consumption of energy is less So our proposed solution works better for larger network which is an advantage by itself.

VI. CONCLUSION

The capacity to detect the legitimate neighbors in wireless network is very important part of many functions of the network. If the network with the presence of attacker fails to detect, could leads to information disclosure, wrong localization, incorrect routing and more importantly adversary nodes can get control over network communication. Our proposed solution works well in finding the various attacker nodes and thus makes a legitimate neighbor communication which eventually increases the performance of the protocol. The simulation results show that algorithm can be applied to larger networks with maximum number of nodes which was a drawback of existing approaches. Our future work includes adding enhancements to the proposed solution for reducing consumption energy.

ACKNOWLEDGEMENT

The authors thank CMR Institute of Technology for the continuous support during the implementation of the proposed work.

VII. REFERENCES

[1]L. Bao and J. J. Garcia-Luna-Aceves. A new approach to channel access scheduling for ad hoc networks. In *ACM MOBICOM*.
[2] C. E. Perkins and E. M. Belding-Royer. Ad-hoc on-demand distance vector routing. In *IEEE WMCSA*, 1999.
[3] D. B. Johnson and D. A. Maltz. Dynamic source routing in ad hoc wireless networks. In *Mobile Computing*, pages 153–181. Kluwer Academic Publishers, 1996.
[4] L. Li, J. Y. Halpern, P. Bahl, Y.-M. Wang, and R. Wattenhofer. A cone-based distributed topology-control algorithm for wireless multihop networks. *IEEE/ACM Transactions on Networking*, 2005.
[5] Y. Hu, D. Johnson, and A. Perrig, and, "Packet leashes: a defense against wormhole attacks in wireless networks" In International Conference on Computer Communications (Infocom), 2003.
[6] Healy.M, Newe.T, Lewis.E, „Security for Wireless Sensor Networks: A Review□, IEEE Sensor Application Symposium, New Orleans, LA, USA-Feb 17-19, 2009.
[7] Raymond, D.R, Midkiff, S.F, „Denial of Service in Wireless Networks: Attacks and Defences, IEEE CS: Security and Privacy, 2008,pg 74-81.
[8] P. P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Capkun, and J.-P. Hubaux, "Secure Neighborhood Discovery: A Fundamental Element for Mobile Ad Hoc Networking," IEEE Communications 2008.
[9] L. Hu and D. Evans,"Using directional antennas to prevent wormhole attacks" in Conference on Mobile Computing and Networking 2004.
[10] R. Stoleru, H. Wu, H. Chenji "Secure Neighbor Discovery in Mobile Ad Hoc Networks" 2011 Eighth IEEE International Conference on Mobile Ad-Hoc and Sensor Systems.
[11] B. Parno, A. Perrig, and V. D. Gligor, "Distributed detection of node replication attacks in sensor networks," in IEEE Symposium on Security and Privacy. IEEE Computer Society, 2005, pp.49-63.Online].Available:http://doi.ieeecomputersociety.org/10.1109/SP.2005.8
[12] Yahaya.F.H, Yussoff.Y.M, Rahman.R.Ab, Abidin.N.H,□Performance Analysis of Wireless Sensor Network□, 5th International Colloquium on Signal Processing & its Applications (CSPA), 2009.
[13] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *the First IEEE International Workshop on Sensor Network Protocols and Applications*, pp. 113–127, May 2003.
[14] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical En-route Filtering of Injected False Data in Sensor Networks," *IEEE INFOCOM*, March 2004.
[15]http://www.ias.ac.in/resonance/July2002/pdf/July2002p35-43.pdf
[16]Introduction to Agents, agents.umbc.edu/introduction/

