Override of Multiple Wormhole Attack in 60GHz Directional Network and Energy Efficiency with LEACH Protocol

N. Sunil, P. Sivaprakash and N.Nalini
PG Scholar, Assistant Professor, Assistant Professor
CSE Department, CSE Department, CSE Department

Abstract--- Overcome of Multiple Wormhole Attack in Wireless Network is a difficult process. In order to overcome from wormhole attack we should go for Secure Neighbor Discovery (SND) scheme. Initialize 60GHZ directional network to minimize the coverage area of Substation through antenna. As we reduce coverage area we can able to easily detect the wormhole attack. Signal and Data Flow Controller (SDFC) is placed in the middle of network. Information transformation between Nodes and SDFC should have high range of security mechanism. Therefore we can go for private/public key Authentication. To overcome Transmission collision the Response/Authentication phase and Low Energy Adaptive clustering hierarchy (LEACH) routing Protocol has been initialized. Introduce SDFC timing phase to recognize multiple wormhole attack in wireless network. The Efficiency of LEACH Protocol is high because the power distribution is properly exhibited to all the nodes. Finding Cluster head will be a complex task to attacker because it will be changing at regular intervals. LEACH protocol has the advantage of reducing power as well as the traffic in wireless transmission.

Index Terms---Directional network, SND scheme, Key authentication, LEACH Protocol

I. Introduction

The wormhole attack has been proposed, a severe attack in networks that is particularly challenging to defend against. The wormhole attack is possible even if the attacker has not compromised any hosts and even if all communication provide authenticity and confidentiality. To overcome real world problems in wireless network we should have attention on industrial and academic projects. Proposing transceiver architecture for Automatic beam forming and instantaneous setup of a multi giga bit-per-second wireless link between two millimeter wave radios. For cost reduction in developing 60GHZ transceivers implement CMOS technologies. Normally in routing and communications focus on security. In order to maintain security in large communication area is highly difficult process.

Therefore splitting the Omni directional network into various divisional networks by using directional antennas is to be carried out. Finding of attacker in Omni directional network is a complicated process were as in divisional network it will be an easier one. Then will be dividing the network into sub divisional by providing beam from SDFC which is provided in middle of the network. The SDFC will be maintaining the frequency and the data transmission to all nodes. By using the digital algorithm will be splitting the network which will be a complicated action. Discovery of neighboring nodes will be an easier process in the divisional networks and also discovery of wormhole attack will be also simple.

For secure transmission we should implement pair of keys which will be known only by the transceiver and receiver nodes. In order to improve the security we will be increasing the key length. As the key size is large it will be difficult for the attacker to analyze the key within particular time. For easier wormhole detection we will be focusing on Time Analysis while broadcasting data from SDFC to all the nodes and for Response/Authentication process has to be enveloped from nodes to the SDFC.

From this we can able to understand that connections between the nodes and SDFC will be in bidirectional. Low Energy Adaptive Clustering Hierarchy (LEACH) is an energy-efficient hierarchical-based routing protocol. Our prime focus was on the analysis of LEACH based upon certain parameters like network lifetime, stability period, etc and also the effect of selective forwarding attack and degree of heterogeneity of LEACH protocol. After a number of simulations, it was found that the stability regions length is considerably increased by choosing an optimal value of heterogeneity; energy is not properly utilized and throughput is decreased in networks compromised by selective forwarding attack but the number of cluster-head spreads round remains unelected in such networks. The main work done on this paper has been summarized below.

- Fist, for attack resistant introducing SND scheme which maintains secure communication between bidirectional connectivity. We utilize key authentication scheme and time analysis for secure transmission and attack identification through broadcasting messages.

- Second, LEACH protocol has been introduced for secure route discovery and maintains energy adopted for the specified actions. Due to proper energy distribution traffic will be easily maintained.
- Third, proposing algorithm for high secure communication and discussion about the effectiveness and energy considerations for the proposed wormhole attack resistant scheme.

The paper has been organized as following in section 2, the problem formulation has been designed for the attack detection in wireless networking and in section 3, proposed network architecture and then in section 4, analyze about beam forming in 60GHZ direction using directional antenna then in section 5, we develop an algorithm for key authentication scheme and in section 6, we emphasize the advantages of utilizing the LEACH protocol in the proposed system in section 7, finally we conclude the paper.

II. Problem Statement

In this section we formulate the design for the attack detection in the wireless network and encapsulate necessary conditions.

A. Network Communication

From the usage of model 802.15.3c and 802.11ad, it is known that all the applications are based on centralized design, i.e., the SDFC will be located in the center of the divisional network and supports for data transmission in concurrent point to point between different pairs of devices. We consider 60GHZ directional network composed of multiple wireless nodes N= {n1, n2, n3…} with single SDFC. Normally the wireless nodes are distributed randomly in a network with density p per square meter. We will be providing L number of beams through directional antenna with angle 2π/L radians.

All beams will be collectively having the same density for coverage area in all directions. The beams are constructed in a clockwise direction. The SDFC use its directional antenna to communicate with other nodes up to the distance R. Transmitter and Receiver are placed in directional antenna with average power. The fig.1 shows the wireless node distribution in the network.

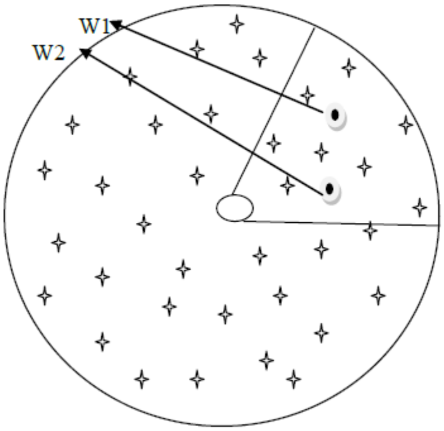

Fig 1 Divisional Network

All the wireless nodes do not have specialized hardware such as a GPS module to know its own global position, but they do have a kind of electronic compass which is much cheaper than the GPS module and used to align the beam direction, i.e., different antennas with the same beam number point to the same sector.

B. Attack Consideration

Wormhole attack is one type of active attack, in which malicious nodes relay packets for two legislate nodes to fool them believing that they are direct neighbors. Normally there are two type of wormhole attack.

1. One type of attack is that there will be one malicious node M1 between the source and the destination node.
2. second type of attack there will be more number of malicious nodes (M1,M2…Mn) located between the source and the destination node

In this paper we are considering the second type of attack in wireless network and to overcome from this we will be going for some assumptions.

C. Assumptions

The main aim of the paper is to override from multiple wormhole attack within the 60GHZ directional network. We should consider some assumptions necessary as follows.

- Assumption1:The SDFC should be considered as the trusted centralizer which will be providing proper authentication, neighbor discovery, malicious node detection, etc

- Assumption2: The key based authentication has been developed for secure communication between SDFC and nodes vice versa. The malicious nodes will be having same power for computation but they will not able to attain the key materials of the legislative nodes.

D. PROPOSED SCHEME FOR WORMHOLE ATTACK RESISTANCE

In this, we proposed the main idea for multiple wormholes resistant in the directional network. As we are finding more difficulties in finding malicious nodes in the Omni directional network we are going for directional network. We will be having three different phases for the project development namely broadcasting phase, response/authentication phase, time analysis phase.

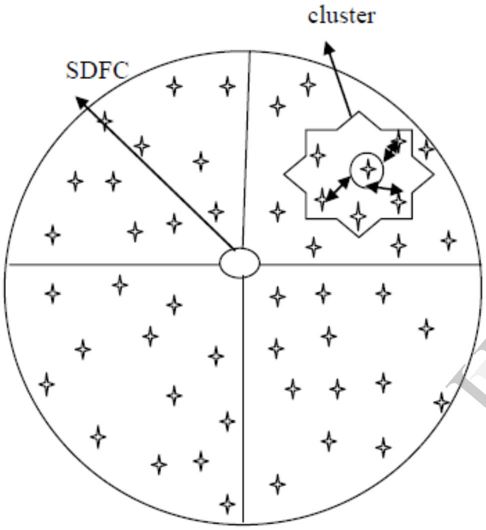

Fig 2 Cluster formation structure

Normally nodes are spread in wireless network. The SDFC will be provided in the middle of the network and it will be connected with the nodes within the 360 degree. Therefore the attack detection is complicated we will split the 360 into eight 60 degree directional network with help of beam construction. Due to this divisional network we can able to easily find out the malicious nodes. Then we will be using the LEACH routing protocol for transmitting data with low energy and with less time. This protocol will be forming a cluster head in the distributed network.

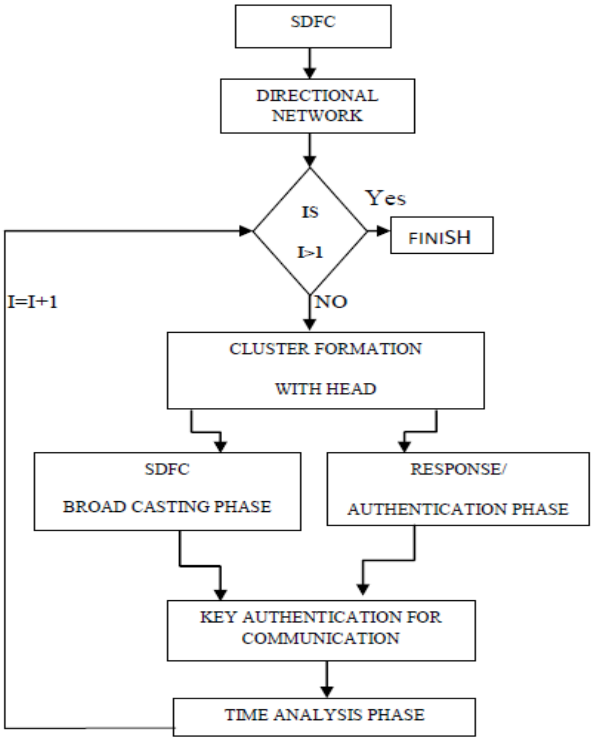
SDFC
DIRECTIONAL NETWORK
IS I>1
Yes
FINISH
NO
I=I+1
CLUSTER FORMATION WITH HEAD
SDFC BROAD CASTING PHASE
RESPONSE/ AUTHENTICATION PHASE
KEY AUTHENTICATION FOR COMMUNICATION
TIME ANALYSIS PHASE

Fig 3 Flow diagram

Before forming the cluster head the base station will be calculating the distance between source and the destination node and according to the distance the cluster head will be allocated.

The cluster head will be broadcasting the hello message to the nodes which has to be bounded to it within a particular directional network. After receiving the message each node will be replying with authentication or response message. The message in bidirectional method should follow the secure key authentication.

For secure communication, will be using the private/public key in both transmitting and receiving side. Therefore the key value will be known only by the transmitting and the receiving node. We will be providing time analysis for response/ authentication phase because according to the time for acknowledgement we can able to recognize the attack in the directional network.

III. CODING FOR WORMHOLE

```
void ProbingTimer::expire(Event*) { t_->timeout();
}
//base class for worm: host is invulnerable by default static class
WormAppClass : public TclClass {
public:
WormAppClass() : TclClass("Application/Worm") {} TclObject*
create(int, const char*const*) {
return (new WormApp());
}
} class_app_worm;
//Initialize static variables
double WormApp::total_addr_ = pow(2, 32); int
WormApp::first_probe_ = 0;
WormApp::WormApp() : Application() {
//get probing rate from configuration bind("ScanRate",
&scan_rate_);
//get probing port from configuration bind("ScanPort",
&scan_port_);
//get probing port from configuration bind("ScanPacketSize",
&p_size_);
}
void WormApp::process_data(int nbytes, AppData* data) {
recv(nbytes);
}
void WormApp::recv(int nbytes) { if (!first_probe_) {
first_probe_ = 1;
printf("D FP %.2f\n", Scheduler::instance().clock());
}
//printf("D U %.2f %d\n",
//Scheduler::instance().clock(), my_addr_);
}
```

When the cluster head gets acknowledgement at proper time from every nodes within the cluster will start to transfer message to the destination nodes though its cluster. Thus the cluster head will be changing for each rotation it will be difficult for the attacker to destroy the node considered as the head of the cluster formation.

IV. ANALYSIS OF BEAM FORMING IN 60GHZ DIRECTIONAL NETWORKS

The demand for high speed wireless communication systems has made it necessary to move to millimeter wave frequencies. The path loss at these frequencies becomes severe as the effective antenna area scales proportionally with the square of wavelength to maintain Omni-directional operation. Thus, use of arrayed antennas providing adaptive beam forming becomes very important. Adaptive beam forming provides high link gains because of antenna directivity, and the radios can conform to different signal directions. Adaptive beam forming requires complex digital algorithms for computing the direction of signal arrival and transmission to set Up a communication link. Even when the radio directions are known, controlling phases of transmit and receive signals to achieve proper directionality becomes difficult.

Exploiting retro directivity to achieve instantaneous link acquisition, in addition to much simpler analog implementation and automatic phasing of the beam forming arrays. A retro directive antenna is an arrayed antenna that transmits in the direction of the incoming electromagnetic signal without prior knowledge of its direction. In the absence of an incoming signal, most of the transmitted power goes Omni-directionally. When a signal is present at the receiver input, power is transmitted in the direction of the incoming signal.

V. KEY AUTHENTICATION SCHEME

In order to set the PKI in the network some distinct features have to be considered based on initialization and maintenance. Before deploying the nodes in the network it should be configured by the base station. Base station will be taking role of initializing and dataflow between the nodes in the network. The base station should be considered as a certification authority. The creation of digital certificate is associated with the identity of node with their public/private key pair. The base station can also create public/private key if the node is not efficient to develop its own key.

According to this project, the SDFC calculates the distance between the source and destination. As per the distance it will be forming the cluster head then it will select some of the nodes into its cluster formation based on the destination node location. Then the broadcasting of message takes place within the cluster formation. As the information reaches the destination node it will send acknowledgement to the source with Response/Authentication field. For both broadcasting and Response/Authentication phase we require secure communication using public/private key authentication. This process to be carried out at each phase of the directional network in order to provide security between communicating nodes.

VI. ADVANTAGES OF UTILIZING THE LEACH PROTOCOL IN THE PROPOSED SYSTEM

Low Energy Adaptive Clustering Hierarchy (LEACH) is an energy efficient hierarchical-based routing protocol. After a number of simulations, it was found that the stability regions length is considerably increased by choosing an optimal value of heterogeneity; energy is not properly utilized and throughput is decreased in networks compromised by selective forwarding attack but the number of cluster-heads per round remains unaffected in such networks.

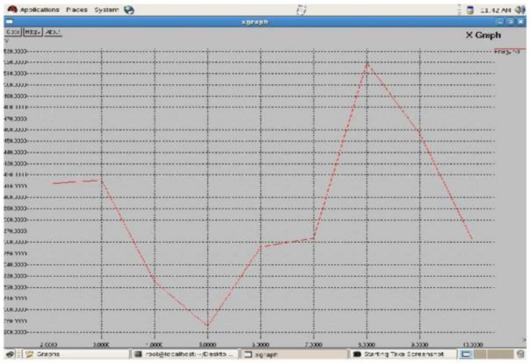

Fig 4 No of cluster heads Vs energy dissipation

Fig 4, X-axis indicates the No. of cluster heads and Y-axis indicates the energy consumed in joules.

LEACH is a hierarchical-based routing protocol which uses random rotation of the nodes required to be the cluster-heads to evenly distribute energy consumption in the network. The development of clustered sensor networks has recently been shown to decrease system delay, save energy while performing data aggregation and increase system throughput.

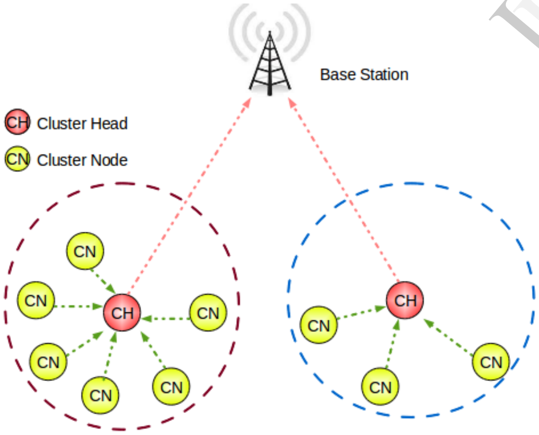

Fig 5 Cluster Head and Base station connection

Also LEACH has a few but very significant disadvantages like it assumes all the nodes to have same energy, which is not the case always in real-time problems, its cannot be applied for mobile nodes, failure of cluster-heads creates a lot of problems and it will not be take into account that the systems might have multiple base stations.

PARAMETERS	VALUES
Distribution area of nodes	100*100
Network monitor area	1000m*1000m
Number of nodes(including base station node)	101
Optimal number of cluster heads	5
Iteration number of the simulated annealing algorithm	1000
Initial energy of node	100J
Wireless communication line bandwidth	1mbps
Time of each round	20s
No of wormhole tunnels	Up to 10 wormholes
Size of packet header	25 Bytes
Data size of packet	500 Bytes
Simulation time	900s
Effusion	5 nJ/bit
Distance threshold d()	70 m

Fig 6 Parameters and Value information

Depending on the protocol operation, routing protocols can be classified into multipath-based. In multipath-based routing, multiple paths are used to enhance network performance i.e. faults tolerance, balance energy consumption, energy-efficiency and reliability.

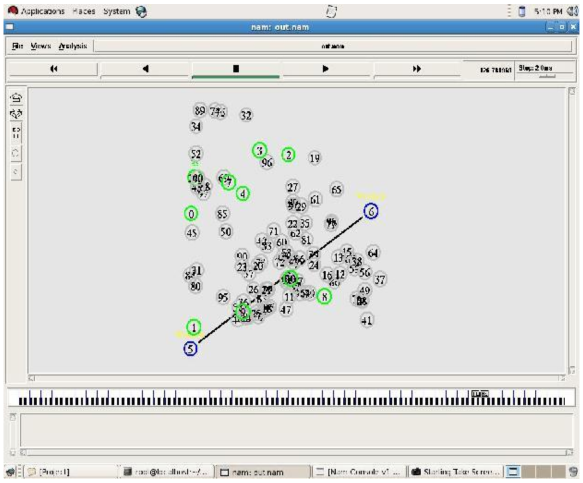

Fig 7 LEAH protocol with worm holes

Fig 7, denotes the wormhole attack in the network. As per the above simulation we calculated the energy dissipation using leach protocol. At this stage we are introducing two nodes as wormhole nodes and calculating the performance with network simulator.

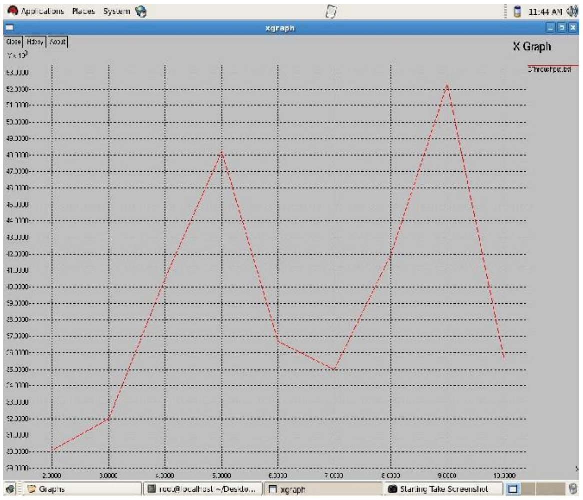

Fig 8 Clusters Vs Lifetime

Fig 8, X-axis indicates the No. of cluster heads and Y-axis indicates the lifetime of network in Milliseconds.

At this stage we will be calculating the lifetime of the cluster nodes. Therefore we are considering the number of nodes in the cluster and the cluster head and noticing the standby period of these nodes using network simulator.

VII. CONCLUSION

According to the proposed system, LEACH protocol will be playing main role. As this protocol follows the cluster based communication the energy utilized for communication will be set lower. To maintain security during the communication, key authentication process has been carried out. The time for acknowledgement simplifies finding of attack in directional wireless network. To design directional network beam forming with help of antenna directivity makes it simple. To develop this proposed system we should consider the SDFC as trust worthy.

VIII. REFERENCE

[1] Z. Shi, R. Lu, J. Chen, and X. S. Shen, "Three dimensional spatial multiplexing for directional millimeter wave communications in multicubicle office environments," in *Proceedings of 2013 Globecom*. IEEE, 2013, pp. 1–6.

[2] Z. Shi, R. Lu, J. Qiao, and X. Shen, "Snd: Secure neighbor discovery for 60 ghz network with directional antenna," in *Proceedings of IEEE WCNC 2013*, pp. 1–6.

[3] S.-R. Lee, S.-H. Moon, J.-S. Kim, and I. Lee, "Capacity analysis of distributed antenna systems in a composite fading channel," *IEEE Trans. Wireless Commun.*, vol. 11, pp. 1076–1086, Mar. 2012.

[4] H. Kim, S.-R. Lee, K.-J. Lee, and I. Lee, "Transmission schemes based on sum rate analysis in distributed antenna systems," *IEEE Trans. Wireless Commun.*, vol. 11, pp. 1201–1209, Mar. 2012.

[5] C. Cordeiro, D. Akhmetov, and M. Park, "Ieee 802.11 ad: introduction and performance evaluation of the first multi-gbps wifi technology," in *Proceedings of the 2010 ACM international workshop on mmWave communications: from circuits to networks*. ACM, 2010, pp. 3–8.

[6] H. Singh, S. Yong, J. Oh, and C. Ngo, "Principles of ieee 802.15. 3c: Multi-gigabit millimeter-wave wireless pan," in *Proceedings of 18th IEEE Internatonal Conference on Computer Communications and Networks*, 2009, pp. 1–6.

[7] S. Vasudevan, J. Kurose, and D. Towsley, "On neighbor discovery in wireless networks with directional antennas," in *Proceedings of IEEE INFOCOM 2005*, vol. 4, 2005, pp. 2502–2512.

[8] An, R. Prasad, and I. Niemegeers, "Impact of antenna pattern and link model on directional neighbor discovery in 60 ghz networks," *IEEE Transactions on Wireless Communications*, vol. 10, no. 5, pp. 1435–1447, 2011.

[9] J. Du, E. Kranakis, and A. Nayak, "Cooperative neighbor discovery protocol for a wireless network using two antenna patterns," in *Proceedings of 32nd IEEE International Conference on Distributed Computing Systems Workshops*, 2012, pp. 178–186.

[10] R. Zhao, A. Wen, Z. Liu, and J. Yang, "A trustworthy neighbor discovery algorithm for pure directional transmission and reception in manet," in *Proceedings of IEEE 9th International Conference on Advanced Communication Technology*, vol. 2, 2007, pp. 926–931.

[11] Ralph Merkle. Protocols for Public Key Cryptosystems. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pages 122–136, April 1980.

[12] David L. Mills. A Computer-Controlled LORAN-C Receiver for Precision Timekeeping. Technical Report 92-3-1, Department of Electrical and Computer Engineering, University of Delaware, Newark, DE, March 1992.

[13] Lingxuan Hu and David Evans. Using Directional Antennas to Prevent Wormhole Attacks. In *Proceedings of the 2004 Symposium on Network and Distributed Systems Security (NDSS 2004)*, February 2004.

[14] Jean-Pierre Hubaux, Levente Butty´an, and Srdjan ˇCapkun. The Quest for Security in Mobile Ad Hoc Networks. In *Proceedings of the 2001 ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2001)*, pages 146–155, October 2001.

[15] Raymond L. Pickholtz, Donald L. Schilling, and Laurence B. Milstein. Theory of Spread Spectrum

Communications—A Tutorial. *IEEE Transactions on Communications*, 30(5):855–884, May 1982.

[16] Radha Poovendran and Loukas Lazos. A Graph Theoretic Framework for Preventing the Wormhole Attack in Wireless Ad Hoc Networks. *ACM Wireless Networks (WINET)*. to appear.

[17] H. Shin, M. Z. Win, J. H. Lee, and M. Chiani, “On the capacity of doubly correlated MIMO channels,” *IEEE Trans. Wireless Commun.*, vol. 5, pp. 2253–2265, Aug. 2006.

[18] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.

[19] G. M. Guvensen and A. O. Yilmaz, “An upper bound for limited rate feedback MIMO capacity,” *IEEE Trans. Wireless Commun.*, vol. 8, pp. 2748–2754, June 2009.

[20] A. A. M. Saleh, A. J. Rustako, and R. S. Roman, “Distributed antennas for indoor radio communications,” *IEEE Trans. Commun.*, vol. 35, pp. 1245–1251, Dec. 1987.