Hello Flood Attack Using BAP in Wireless Sensor Network

Gayatri Devi[1], Rajeeb Sankar Bal[2], Nibedita Sahoo[3]

[1]Professor, Department of CSE, Ajay Binay Institute of Technology,Cuttack -753014,Odisha
[2]Senior Lecturer, Department of CSE, Ajay Binay Institute of Technology,Cuttack -753014,Odisha
[3]M.Tech(CSE) Student, Department of CSE, Ajay Binay Institute of Technology,Cuttack -753014,Odisha

Abstract— *A wireless sensor network is a network of numerous sensing nodes that execute a certain task .The network can consist of any number of sensing nodes, and each sensor node has the ability to store and send information across the network. An attacker can eavesdrop on messages posted by any sensor node; security is an important issue here. In this paper, we consider Wireless Sensor Network security and focus our attention to tolerate harm caused by an adversary who has compromised deployed sensor node to change, block, or inject packets. We then analytically show that our defense mechanisms against HELLO Flood attack using BAP Method.*

Keywords—Wireless Sensor Network (WSN), Flooding, Cryptography, Puzzle, Signal Strength (SS).

I. INTRODUCTION

A WSN is a collection of nodes organized into a cooperative network. Each node consists of processing capacity (one or more microcontrollers, CPUs or DSP chips), contain multiple types of memory (program, data and flash memories), have a RF transceiver (usually with a single Omni-directional antenna), have a power source (e.g., batteries and solar cells), and accommodate various sensors and actuators. The nodes communicate wirelessly and frequently self-organize after being deployed in an ad hoc fashion. Systems of 1000s or even 10,000 nodes are anticipated [1]. Such systems can modernize the way we live and work.

Currently, WSNS are beginning to be deployed at an accelerated pace [1]. It is not difficult to expect that in 10-15 years that the world will be covered with WSNs with access to them via the Internet. This can be well thought-out as the Internet becoming a physical network. This new technology is exciting with unrestricted potential for several application areas including environmental, medical ,military ,transportation, crisis management, entertainment, homeland defense and smart spaces.

II. WSN SECURITY ANALYSIS

Simplicity in WSN with resource constrained nodes makes them extremely susceptible to variety of attacks. Attackers can eavesdrop on our radio transmissions, infuse bits in the channel, replay previously heard packets and many more. Securing the WSN needs to construct the network support all security properties: confidentiality, integrity, authenticity and availability. Attackers may deploy a few malicious nodes with similar hardware capability as the legitimate nodes that might collude to attack the system helpfully. The attacker may come upon these malicious nodes by purchasing them separately, or by "turning" a few legitimate nodes by capture them and physically overwriting in their memory. Also, in some cases colluding nodes might have high-quality communications links available for coordinating their attack. Sensor nodes may not be tamper resistance and if an adversary compromise a node, she can extract all key objects, data, and code stored on that node. While tamper resistance might be a feasible defense for physical node compromise for some networks, we do not see it as a general purpose solution. Extremely effective tamper resistance tends to add significant per-unit cost, and sensor nodes are proposed to be very cheap [2].

ATTACKS AT DIFFERENT LAYER

These attacks take place disturbing different networking layers of WSN. This section describes some of these well known attacks.

1) Physical Layer

Physical layer is responsible for actual data transmission and receipt, frequency selection, carrier frequency generation, signaling function and data encryption [3]. This layer also address the transmission media among the communicating nodes. WSN uses shared and radio based transmission medium which make it susceptible to radio interference or jamming .

1.1) Jamming

Jamming is a common attack in physical layer, that can be easily done by adversaries by only knowing the wireless transmission frequency used in the WSN [4]. The attacker transmits radio signal at random with the same frequency as the sensor nodes are sending signals for communication. This radio signal interfere with other signal sent by a sensor node and the receiver contained by the range of the attacker cannot receive any message.

2)Data Link Layer

The data link layer is responsible for the multiplexing of data streams, data frame detection, medium access and error control. This layer is vulnerable to data collision when number of sender tries to send data on a single transmission channel.

2.1) DoS Attack by Collision Generation

In data link layer, collision is generated to weaken the sensor node's energy. In order to generate collision, the attacker listens to the transmissions in WSN. When he finds out the starting of a message, he sends his own radio signal for a small amount of time to interfere with the message which causes CRC error at the receiving end. The receivers cannot receive the message correctly, because of this attack.

3) Network Layer

Network layer is responsible for routing messages from one to another node which are neighbours or may be multi hops away. For example, node to base station or node to cluster leader. The network layer for WSN is usually planned taking into consideration the power efficiency and data centric characteristics of WSN. There are several attacks exploiting routing mechanisms in WSN. Some well-known attacks are listed below.

3.1) Selective Forwarding

Selective forwarding is an attack where malicious node just drops packets of its interest and selectively forwards packets to minimize the mistrust to the neighbour nodes. The impact becomes worse when these malicious nodes are at nearer to the base station [4]. Then many sensor nodes route messages through these malicious nodes. As a effect of this attack, a WSN may give wrong observation about the environment which affects badly the purpose of mission critical applications such as, military surveillance and forest fire monitoring.

3.2) Sinkhole attack

In sinkhole attack, a compromised node attracts many number of traffic of surrounding neighbours by spoofing or replaying an announcement of high quality route to the base station [4]. The attacker can do any malicious action with the packets passing through the compromised node.

3.3) Wormhole Attack

Wormhole is a crucial attack, where the attacker receives packets at one point in the network, tunnels them through a less latency link than the network links to another point in the network and replay packets there locally [4]. This convinces the neighbour nodes of these two end points that these two distant points at either end of the tunnel are very close to each other. If one end point of the tunnel is at near to the base station, the wormhole tunnel can attract considerable amount of data traffic to disrupt the routing and operational functionality of WSN. In this case, the attack is similar to sinkhole as the adversary at the other side of the tunnel advertise a better route to the base station.

3.4) Sybil Attack

In Sybil attack, a malicious node forge the identities of more than one node or fabricates identity. This attack has important effect in geographic routing protocols [4]. In the location based routing protocols, nodes need to exchange location information with their neighbours to route the geographically addressed packets efficiently. Sybil attack disrupts this protocol functionality simultaneously being at more than one place. Identity verification is the key requirement for countering against Sybil attack. Unlike traditional networks, verification of identity in WSN cannot be done with a single shared symmetric key and public key algorithm because of computational limitation of WSN.

4) Transport Layer

In transport layer end to end connections are managed. Unlike traditional networks, protocols like TCP where the end-to-end communication schemes are possible, here there is no global addressing. The development of global addressing schemes is still a challenge.

4.1) Flooding Attack

According to, at this layer this layer, adversaries utilize the protocols that maintain state at either end of the connection.For example, adversary sends many connection establishment requests to the victim node to drain its resources causing the Flooding attack. One solution against this attack is to limit the number of connections that a node can make. But, this can prevent legitimate nodes to connect to the victim node.

4.2)Hello Flood Attack

An attacker sends or replays a routing protocol's HELLO packets from one node to another with more energy. This attack uses HELLO packets as a weapon to convince the sensors in WSN. In this type of attack an attacker with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes that are isolated in a large area within a WSN. The sensors are thus influenced that the adversary is their neighbor. As a result, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbour and are ultimately spoofed by the attacker.[4]

5.) Application Layer

Also not available. Although there are many application areas for sensor networks, application layer protocols are yet to be developed.

Table
Different layer attack and defences

Layer	Attacks	Defenses
Physical	Jamming	Spread-spectrum, priority messaging, lower duty cycle, region mapping, mode change
	Tampering	Tamper-proof, hiding
Data link	Collision	Error correcting code
	Exhaustion	Rate limitation
	Unfairness	Small frames
Network	Neglect and grid	Redundancy, probing
	Homing	Encryption
	Misdirection	Egress filtering, authorization monitoring
	Black holes	Authorization, monitoring, redundancy
Transport	Flooding	Client puzzles,Broadcast Authentication Puzzle
	Desynchronization	Authentication

III. HELLO FLOOD ATTACK

In a HELLO flood attack a malicious node can send, record or repeat HELLO-messages with high transmission power. It creates an illusion of being a neighbor to many nodes in the networks and can confuse the network routing badly. This attack is based on the use by many protocols of broadcast Hello messages to announce themselves in the network. So an attacker with greater range of transmission may send many Hello messages to a large number of nodes in a big are a of the network[7]. These nodes are then convinced that the attacker is their neighbor. So that all the nodes will respond to the HELLO message and waste their energy. Consequently the network is left in a state of confusion.

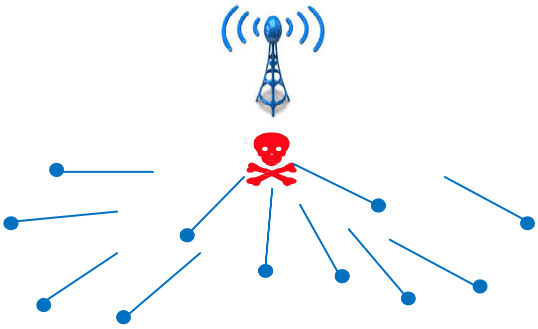


Fig 1 Hello Flood Attack

Some routing protocols in WSN require nodes to broadcast hello messages to announce themselves to their neighbours. A node which receives such a message may assume that it is within a radio range of the sender. However in some cases this assumption may be false; sometimes a laptop-class attacker broadcasting routing or other information with large enough transmission power could convince every other node in the network that the attacker is its neighbour. For example, an adversary advertise a very high quality route to the base station could cause a large number of nodes in the network to attempt to use this route. But those nodes which are sufficiently far away from the adversary would be sending the packets into oblivion. Hence the network is left in a state of confusion. Protocols which depend on localized information exchange between neighbouring nodes for topology maintenance or flow control are mainly affected by this type of attack.[5]An attacker does not necessarily need to construct legitimate traffic in order to use the hello flood attack. It can simply re-broadcast overhead packets with enough power to be received by every other node in the network.[5]

Hello Packet Properties

There are five main features of hello packet are given below [6]

1) The size of Hello packet is small as compared to data packet.

2) The probability of hello flood reaching to its receiver is higher than data packet especially over weak links.

3) Broadcasting of Hello packet is always done at basic bit rate because Lower bit rate transmission is more reliable.

4) Hello packets are broadcasted without any acknowledgement.

5) There is no guarantee about the bidirectional communication of hello packets.

IV. DEFENCE STRATEGIES AGAINST HELLO FLOOD ATTACK

In this section I present security schemes against hello flood attack using cryptographic schemes. In this paper we have proposed a solution for detection of hello flood attack which is based on signal strength and broadcast authentication puzzles method.

Signal strength of all sensor nodes is assumed to be same in a radio range. Each node checks the signal strength of the received hello messages with respect to known radio range strength; if they are same then sender node is classified as a “friend” else sender is classified as a “stranger”. When any node is classified as a stranger, we try to check its validity using some broadcast authentication puzzles.

Some primary assumption are-

(1) Communication is within fixed radio range.

(2) All sensor nodes in a fixed radio range have same transmitting and receiving signal strength.

(3) All sensor nodes are homogeneous (same hardware and software, battery power etc.).

(4) Every sensor node knows the fixed signal strength used in its communication range.

(5) A time threshold is used, which denotes the expected time of reply message.

(6)Synchronized Clock of sender and receiver.

(7) A hello message counter has been used by all sensors to keep the record of number of hello requests received in an allotted time.

Initially signal strength is calculated as two ray propagation model [6]

$$P_r = (P_t * g_t * g_r * h_r^2 * h_t^2)/(d^4 * L) \qquad (1)$$

In eq. 1 Pr is received signal power (in watts), Pt is transmission power (in watts), G_r is the transmission antenna gain, G_r is the receiver antenna gain, Ht is the transmitter antenna height (in meter) and Hr is the receiving antenna height(in mete), d is the distance between transmitter and receiver (in meter), and L is the system loss(a constant). A signal is only detected by a receiving node if the received signal power Pr is equal or greater than the received signal power threshold Pthres. When any laptop class attacker sends hello message to a legitimate node in a fixed radio range then the receiving node checks its hello message signal strength, if it is same then requesting node is a legal node of the network; if it differs, it categorizes the sender node as stranger.

Signal strength = Fixed signal strength in radio range=friend

Signal strength > Fixed signal strength in radio range=stranger

Authentication using one Way Chain and Delay key

The basic idea is as follows:

➢The sender creates a hash chain by selecting a random element H_0 as root and by iteratively applying to it a one way function F. This produces the sequences $H_0\ H_1 \cdots\cdots\cdots\cdots\ H_n$ where $H_i = F^i(H_0)$, for $1 \le i \le n$.

➢As F is one way function, a receiving node possessing H_i cannot feasibly calculate the predecessor H_{i-1},only owner of the root can calculate, by computing forward from H_0.

➢We define F =x ⊕ y, H_i=F ⊕ H_i

➢We use ⊕ operation for one way hashing.

➢Given a string s, any node possessing H_i can easily check if $s = H_{i-1}$ by checking if F(s)=H_i.

➢The sender then commits to hash chain by distributing H_n in an authentic way to the receiver.

➢The receiver synchronizes his clock with the sender at this point.

➢For each H_i, we apply another one way function $F'_{n-(i-1)}$ to derive a key K'_{n-1}, for the corresponding time interval n-i.

➢ Is used to avoid using the string H_i for 2 different purposes:- as a hash value in the chain and as a key.

➢To authenticate a messages m, the sender assigns the message to a time interval.

➢To send m in the (n — i)th time interval, the sender appends to m a keyed MAC,$MAC_{k_{n-i}}(m)$,as well as the chain element for the preceding time interval, H_{i+1} , using sha-1 algorithm.

➢This hash value opens the commitment to, H_{i+1} and hence the receiver can determine the key $K_{n-(i+1)}$ and thereby authenticate the previous message.[8]

➢Then we send message encrypting it with RSA algorithm.

Example:

As mentioned above by considering

$1 \le i \le 3$

$H_i = F^i \oplus (H_0)$Hence,

$H_1 = F^1 \oplus (H_0), H_2 = F^2 \oplus (H_0),$

$H_3 = F^3 \oplus (H_0)$

String, $s = H_1$ F(H_1)=H_2 $s = H_2$,F(H_2)=H_3

$\text{key at receiver} F'_{n-(i-1)} = K'_{n-1,}\ s = K_{n-(i-2)}$

, n=4

Broadcast Authentication using Cryptographic Puzzles

- We assume that the sender and the receivers have synchronized clocks.
- We further assume that a broadcasting node (A) has generated a one-way (hash) chain and distributed its corresponding commitment to the designated receivers (B) in an authentic manner as described above.

BAP-1

BAP-1[8] is designed to achieve instantaneous message verification upon message receipt.

Sender:

- Sender first chooses the cryptographic key K_i, which corresponds to the time interval i = [t_i , t_{i+1}[(where [t_i , t_{i+1} [denotes the set {t ⊂R | t_i ≤ t < t_{i+1} })]]
- The sender then encapsulates K_i, within a cryptographic puzzle Puzzle(K_i), and broadcasts the puzzle at time $t^{A}_{s_0}$. The puzzle serves to hide the key for a given time(which depends on the puzzle complexity and on the solver's processing speed.
- Immediately after the last bits of the puzzle have been sent (at $t^{A}_{s_n}$), the sender starts transmitting the message

authentication code MAC_{k_i}(m), computed over the broadcast message m, using the key K_i contained in the puzzle.

- When the last bits of MAC_{k_i}(m),are sent (at $t^{A}_{s_x}$), the sender transmits the broadcast message m.

Receiver:

- At time $t^{B}_{r_1}$, the receiver B receives the puzzle Puzzle′ and starts solving it to retrieve the key K_i ′.(Here, all messages received by B are marked with ’ to denote that they may have been modified in transit by the adversary.)
- To solving the puzzle, B receives MAC′ and subsequently the message m′.
- To verify the authenticity of the message immediately upon its receipt, the receiver must solve the puzzle before receiving the last bits of the message (i.e., prior to $t^{B}_{r_x}$).
- After the receiver solves the puzzle, he then verifies if M AC’ was received within the time interval i.
- If the key K_i ' is indeed authentic and corresponds to the current time slot i and to the claimed sender A.
- If the message authentication code MAC_{k_i}(m)′, computed with the derived key over the received message equals the received authentication code MAC′. If all verifications succeed, then the receiver concludes that the message m′ = m is both authentic (i.e., generated by the claimed source A) and T-recent (i.e., has been sent by A within T time units before reception, where T ≤| $t^{B}_{r_x} - t_i$ |). Hence,the receiver concludes that the message is T-authentic.

BAP-2

BAP-2 is based on an approach similar to BAP-1 using late key disclosure is achieved by use of cryptographic puzzles. The main difference is that, in BAP-2[8], the key, the message and its MAC is encapsulated within it. The puzzle achieves broadcast authentication through delayed key release based on cryptographic puzzles. Message authentication is achieved if the receiver receives the puzzle before the attacker has solved it. All messages received by B are marked with ′ to denote that they might have been modified in transition by the adversary.

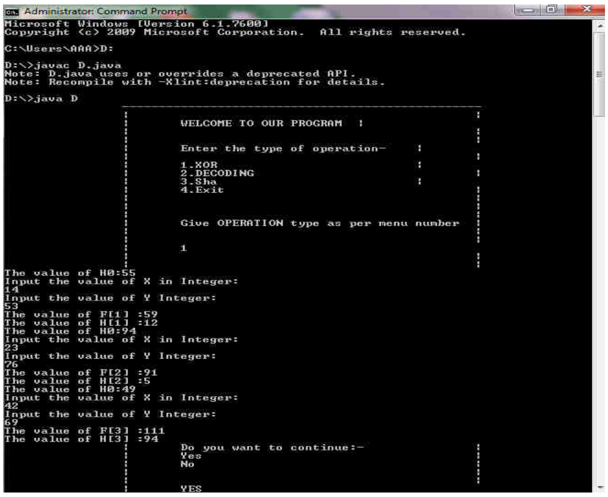
This collapses three messages into one and also reduces the time that the attacker has to solve the puzzle in order to break the scheme. BAP-2 puzzle the sender generates the key for time interval i. Hence the sender encapsulates the message m, its message authentication code MAC, message (m), and the key K_i in a puzzle Puzzle(Puzzle, MAC, m). After receiving the puzzle Puzzle′, the receiver solves it and then verifies that the Puzzle′ was received during the time interval i, that the key K_i (derived from Puzzle′) is indeed authentic and that it corresponds to the current time slot i and to the claimed sender A, the message authentication code M AC’ derived from the puzzle corresponds to M AC′(m′) computed with the derived key K_i over the derived message m′. If and only if all three verifications succeed, the receiver concludes that the message m′ = m is both authentic (i.e., generated by the claimed sourceA) and T-recent (where T Consequently, BAP-2 reaches T-authentication)

One advantage of BAP-2 over BAP-1 is that the attacker has less time to solve the puzzle. Namely, as soon as the first bits of the puzzle are received by the receiver, the attacker looses the possibility to forge the message. Therefore, the key validity time intervals can be shortened in BAP-2 with respect to the intervals in BAP-1, assuming the same message size, key size, and propagation delays. One drawback of this solution is the loss of instantaneous message verification and the inability to prepare the puzzles beforehand (unless the messages are largely predictable or drawn from a small, well-defined set)[8].

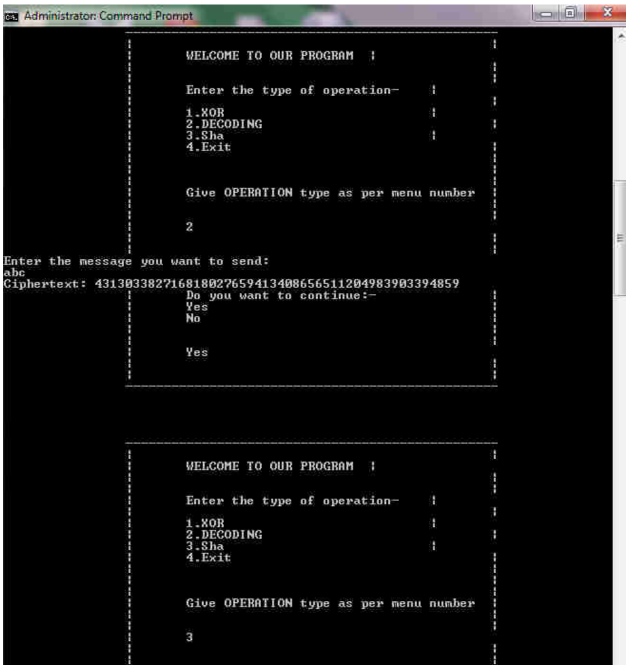
The security analysis of BAP-2 closely resembles that of BAP-1 and we therefore omit further details. Similar to BAP-1, we require that the attacker cannot generate a valid message prior to solving the puzzle and cannot solve the puzzle before the validity of the key expires.

V. RESULT ANALYSIS

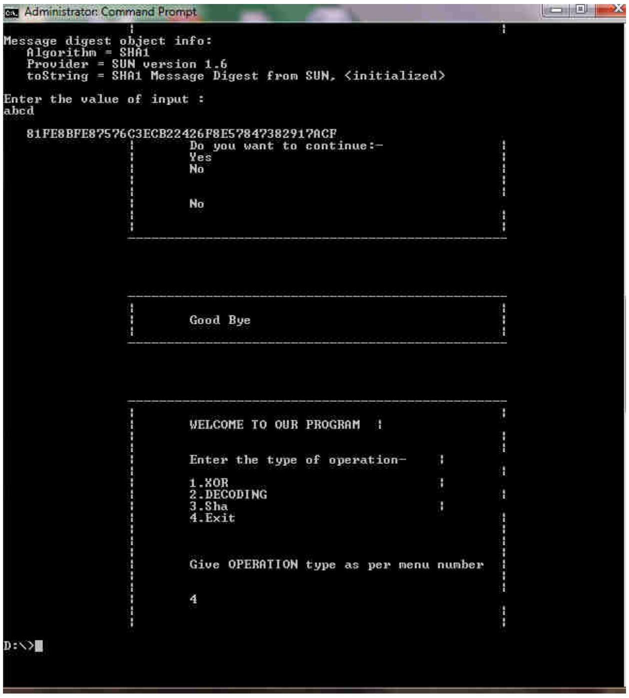
The Coding Result Of BAP-1 Method is as follows



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\AAA>D:

D:\>javac D.java
Note: D.java uses or overrides a deprecated API.
Note: Recompile with -Xlint:deprecation for details.

D:\>java D
                ------------------------------------------------
                |        WELCOME TO OUR PROGRAM  |              |
                |                                               |
                |        Enter the type of operation-    |      |
                |                                               |
                |        1.XOR                           |      |
                |        2.DECODING                             |
                |        3.Sha                           |      |
                |        4.Exit                                 |
                |                                               |
                |        Give OPERATION type as per menu number |
                |                                               |
                |        1                                      |
                |                                               |
The value of H0:55
Input the value of X in Integer:
14
Input the value of Y Integer:
53
The value of F[1] :59
The value of H[1] :12
The value of H0:94
Input the value of X in Integer:
23
Input the value of Y Integer:
76
The value of F[2] :91
The value of H[2] :5
The value of H0:49
Input the value of X in Integer:
42
Input the value of Y Integer:
69
The value of F[3] :111
The value of H[3] :94
                |        Do you want to continue:-              |
                |        Yes                                    |
                |        No                                     |
                |                                               |
                |        YES
```



```
                  WELCOME TO OUR PROGRAM  !

                  Enter the type of operation-    !

                  1.XOR                           !
                  2.DECODING
                  3.Sha                           !
                  4.Exit


                  Give OPERATION type as per menu number


                  2

Enter the message you want to send:
abc
Ciphertext: 4313033827168180276594134086565112049839033948 59
                  Do you want to continue:-
                  Yes
                  No


                  Yes




                  WELCOME TO OUR PROGRAM  !

                  Enter the type of operation-    !

                  1.XOR                           !
                  2.DECODING
                  3.Sha                           !
                  4.Exit


                  Give OPERATION type as per menu number


                  3
```

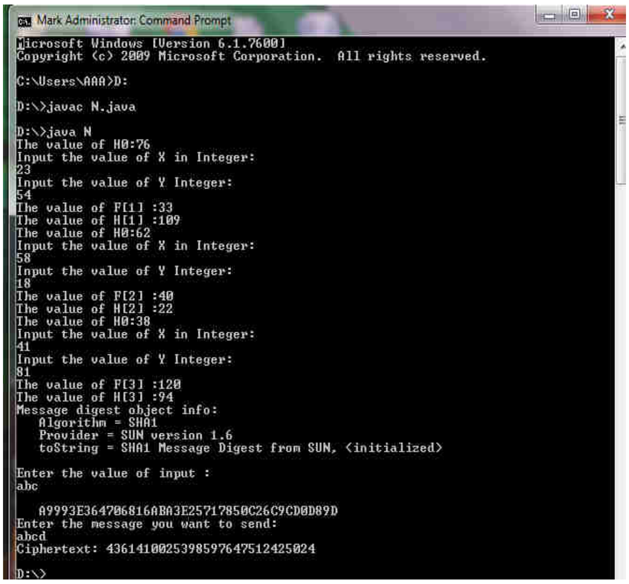


```
Message digest object info:
   Algorithm = SHA1
   Provider = SUN version 1.6
   toString = SHA1 Message Digest from SUN, <initialized>

Enter the value of input :
abcd

   81FE8BFE87576C3ECB22426F8E57847382917ACF
                  Do you want to continue:-
                  Yes
                  No


                  No




                  Good Bye




                  WELCOME TO OUR PROGRAM  !

                  Enter the type of operation-    !

                  1.XOR                           !
                  2.DECODING
                  3.Sha                           !
                  4.Exit


                  Give OPERATION type as per menu number


                  4

D:\>
```

In this coding we use menu sequentially for doing operations and H_0 value is a random number between 1 to 100.

BAP-2

The Coding Result Of BAP-2 Method is as follows.The code for BAP-2 is similar as BAR-1 as it uses same mechanism only key.MAC and message sent at a time.



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\AAA>D:

D:\>javac N.java

D:\>java N
The value of H0:76
Input the value of X in Integer:
23
Input the value of Y Integer:
54
The value of F[1] :33
The value of H[1] :109
The value of H0:62
Input the value of X in Integer:
58
Input the value of Y Integer:
18
The value of F[2] :40
The value of H[2] :22
The value of H0:38
Input the value of X in Integer:
41
Input the value of Y Integer:
81
The value of F[3] :120
The value of H[3] :94
Message digest object info:
   Algorithm = SHA1
   Provider = SUN version 1.6
   toString = SHA1 Message Digest from SUN, <initialized>

Enter the value of input :
abc

   A9993E364706816ABA3E25717850C26C9CD0D89D
Enter the message you want to send:
abcd
Ciphertext: 43614100253985976475124250 24

D:\>
```

VI. CONCLUSION

Security plays a crucial role in the proper functioning of wireless sensor networks. Hello flood attack is the main attack on wireless sensor network, so it is necessary to defend this attack with light and powerful defense schemes. So in this paper we present the hello flood attack, hello packet and cryptographic schemes, signal and puzzle based security scheme and defense schemes of supporting attacks. Our proposed security framework for hello flood detection via a signal strength and cryptographic puzzle method is more secure and hence it is quite suitable for sensor networks. We implement these security schemes on programming to check result and effectiveness in securing sensor networks. In future we can implementing the proposed
scheme in ns-2 to check its effectiveness in securing
sensor networks and other puzzle method.

REFERENCES

[1]Wireless sensor network security: A survey. Security in Distributed, Grid, and Pervasive Computing, 2006. Datema. A Case Study of Wireless Sensor Network Attacks. Master's thesis, Delft University of Technology, September 2005.

[2]WIRELESS SENSOR NETWORK SECURITY ANALYSIS Hemanta Kumar Kalita1 and Avijit Kar2 1Department of Computer Engineering, Jadavpur University, Kolkata, India hemanta91@yahoo.co.in 2Department of Computer Engineering, Jadavpur University, Kolkata, India avijit.kar@gmail.com

[3]A Review on Security Issues in Wireless Sensor Networks Deepika Thakral Neha Dureja Department CSE ,MMU Mullana Department CSE ,MMU Mullana Haryana, India. Haryana, India.

[4]A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks Dr. G. Padmavathi, Prof and Head, Dept. of Computer Science, Avinashilingam University for Women, Coimbatore, India ganapathi.padmavathi@gmail.com Mrs. D. Shanmugapriya, Lecturer, Dept. of Information Technology, Avinashilingam University for Women, Coimbatore, India, ds_priyaa@rediffmail.com

[5]A Survey in Hello Flood Attack in Wireless Sensor Networks Akhil Dubey, Deepak Meena, Shaili Gaur M.Tech. Scholars, Dept. of Computer Science & Engg. IEC-College of Engineering & Technology Greater Noida, U.P., INDIA

[6]Hello Flood Attack and its Countermeasures in Wireless Sensor Networks Virendra Pal Singh1, Sweta Jain2 and Jyoti Singhai3 1 Department of Computer Science and Engineering, MANIT Bhopal, M.P., India 2 Department of Computer Science and Engineering, MANIT Bhopal, M.P., India 3 Department of Electronic and Telecommunication, MANIT Bhopal, M.P., India

[7]Defense Mechanisms against Hello Flood Attack in Wireless Sensor Network Siddhartha Choubey1, Abha Choubey2 , M.Abhilash3 , Kamal K Mehta4 siddhartha00@rediffmail.com niceabha1@rediffmail.com , abhilash576@gmail.com , kkmehta28@yahoo.com ,1 Reader, CSE Dept, SSCET, Bhilai 2 Sr. Lecturer, CSE Dept, SSCET, Bhilai 3ISTE member , CSE, SSCET, Bhilai 4 Asstt.Professor,CSE , SSCET , Bhilai

[8]BAP: Broadcast Authentication Using Cryptographic Puzzles* Patrick Schaller, Srdjan Capkun, and David Basin Computer Science Department, ETH Zurich ETH Zentrum, CH-8092 Zurich, Switzerland {pa1:rick. schaller, srdjan. capkun, david.basin}@in£ . ethz . ch