Journal of Network and Innovative Computing
ISSN 2160-2174 Volume 2 (2014) pp. 001-009

TAWSN - Three-Layered Authentication in Wireless sensor Network

Ambika.N[1] and G.T.Raju[2]

[1] Dayananda Sagar College of Engg, Bangalore
Research Scholar of Bharathiar university
ambika.nagaraj76@gmail.com

[2] Prof & Head, Dept of CS & Engg
RNSIT, Bangalore
drgtraju_rnsit@yahoo.com

***Abstract*: Tiny nodes capable of sensing the environment have become one of the popular trends in surveillance. Sensors are devices which are utilized in innumerable number of applications. These applications vary in size and functionality. Low cost of these motes makes them more liable to different types of attacks. Hence security becomes one of the primary necessities. To defend the network against such type of attacks, prevention and detection techniques come handy.**

This paper adopts a simple analysis which can be adopted in applications which require less amount of security. In this paper, three-layer authentication is performed to secure the network from different attacks. The paper adopts cluster-based routing. The analysis is done at the cluster level and based on the data obtained from the sensors, the base station performs comparative analysis, to analyze compromise node in the network. This approach secures nodes from Sybil attack by 34%, Wormhole attack by 27.8% and Sinkhole attack by 29.8%.

***Keywords*:** Wireless Sensor Network, Intrusion Prevention and detection, Key Distribution

I. Introduction

Wireless sensor network consists of hundreds to thousands of nodes that collaborate to bring the network in to working state. The node in the network sense the environment, records readings and forwards it to the base station. These networks are being utilized in number of applications [1-4] including habitat monitoring [23, 24], battle field surveillance, health care monitoring [20, 21, 22] etc. the level of security varies from one application to another. Military application requires high security, as the data being transmitted are liable to be intruded very often. Other applications like environmental monitoring, intelligent building, and facility management precision agriculture require less security walls to protect the data.

Transmitted data can be secured utilizing two techniques, one being intrusion prevention and other being intrusion detection. Intrusion prevention techniques can be incorporated by encrypting data, authenticating the nodes utilized, filtering what has to be received/ what has to be sent.

Any preventive technique utilized, can tolerate the intrusion to certain extent and hence to secure the system better, additional techniques have to be adopted. Intrusion detection techniques [5 -10] can be divided in to misuse detection and anomaly detection. Misuse detection makes a comparison to the existing database, to detect an attack. The detection technique detects the known attack accurately but cannot trace the emerging attacks. Anomaly detection technique defines a set of parameters for normal circumstances such as CPU utilization, memory utilization etc. when an event occurs, and these parameters are utilized to make a comparison. When a deviation is observed, the node is concluded to be attacked.

Usually the systems are designed, considering types of attack [11, 12] and its frequency in to account. There can be possibility, where in the frequency increases if the adversary is very keen in procuring the restricted data. Hence some mechanism has to be adopted in order to notify the sensors to change their encryption key based on the frequency to attacks. Intrusion detection is one technique, that unearths the abnormal behavior of the system and intrusion prevention is other technique which prevents access to unauthorized data. Combining both the techniques, would significantly improve security of the data.

This paper utilizes additional security compared to existing methods. The work is being considered for the following applications –

- *Environmental monitoring* where lots of chemicals dumped en-route which proves hazardous to plant and

animal life. It can create multiple disorders (water pollution, air pollution etc) to animal and human life.
- *Facility management* where a person is authenticated before he/she enters a particular area of a large organization.

- *Machine surveillances and preventive maintenance* where sensor nodes are fixed in areas of machinery (difficult to reach) to detect vibration pattern that indicate the need for maintenance.

- *Precision agriculture* where the sensors provide precise irrigation and fertilization techniques by checking the humidity/soil composition in the agricultural field.

This paper utilizes anomaly intrusion detection technique [13, 17-19] which is based on simple and resource limited wireless sensor network. Each sensor node maintains a statistical model of the neighboring nodes and triggers the occurrence of abnormal behavior. The IDS agent sends the report periodically to the base station on regular basis. Based on these report reading, the base station broadcasts the message to change the encryption key.

A. Brief Contributions

Security becomes one of the essentials when the network is installed in hostile environment. This approach takes care of the network by monitoring the activities of the nodes, authenticating the data sent and encrypting the data to provide additional precautions. The main contributions are-

- Homogenous network is deployed which takes care of sensing activities, sending the aggregated data to the base station.

- The cluster head is chosen taking the maximum energy stored in the cluster members, proximity and the probability factor. The data sensed by the clustered members is aggregated by the cluster head and forwarded to the base station.

- The cluster head randomly chooses an encryption key and sets the intensity with which the cluster members have to transmit the data. The intensity of the cluster in the transmission mode is altered every time and is checked for correctness.

- The node in the cluster is elected by the base station to monitor, which registers the unusual activity of the network and transmit's the report to the base station.

II. Related work

[14] Presents an intrusion detection model based on hierarchical structure in wireless sensor network. The model structure is simple and improves the security of wireless sensor networks; this model uses a multi-node with the idea of joint collaboration, intrusion detection nodes with anomaly detection algorithm. It shows through experiments with real data that the algorithm can lower the power consumption.

[15] Propose two approaches to improve the security of clustering-based sensor networks: authentication-based intrusion prevention and energy-saving intrusion detection. In the first approach, different authentication mechanisms are adopted for two common packet categories in generic sensor networks to save the energy of each node. In the second approach, different monitoring mechanisms are also needed to monitor cluster heads (CHs) and member nodes according to their importance. When monitoring CHs, member nodes of a CH take turns to monitor this CH. This mechanism reduces the monitor time, and therefore saves the energy of the member nodes. When monitoring member nodes, CHs have the authority to detect and revoke the malicious member nodes. This also saves the node energy because of using CHs to monitor member nodes instead of using all the member nodes to monitor each other. .

[16] Hybrid security system, called energy efficient hybrid intrusion prohibition (eHIP) system, combines intrusion prevention with intrusion detection to provide an energy-efficient and secure cluster-based WSN (CWSN) is proposed. The eHIP system consists of authentication-based intrusion prevention subsystem and collaboration-based intrusion detection subsystem. Both subsystems provide heterogeneous mechanisms for different demands of security levels in CWSN to improve energy efficiency. In authentication-based intrusion prevention, two distinct authentication mechanisms are introduced to verify control messages and sensed data to prevent external attacks. These two authentication mechanisms are customized according to the relative importance of information contained in control messages and sensed data. However, because the security threat from compromised sensor nodes cannot be fully avoided by authentication based intrusion prevention, collaboration-based intrusion detection subsystem is therefore proposed. In collaboration based intrusion detection subsystem, the concept of collaborative monitoring is proposed to balance the tradeoffs between network security and energy efficiency.

III. Preliminaries and notations used

Definition1 (Random Key Distribution): Consider the set of key identifiers $I = \{id_i \mid 1 = i = K\}$ each of which is defined as $id_i = f(k_i)$ where ki is a key chosen at random from a key pool P with $|P| = K$, and f is an arbitrary bijective function. Let K and I be collections of subsets of key pool P and I, respectively. Let $R = \{(R, I) \mid R \in K \text{ and } I \in I\}$ denote the set of collection of key rings. Then, node u will choose a $R_u \in K$, $|R_u| = k$, randomly and uniformly (thus there may exist $R_u = R_v$ for some u = v). Thus, each node contains a set of keys R_u and is identified by $I_u = \{id_i \mid k_i \in R_u\}$.

Notation	Meaning
CH	Cluster Head
C_N	Cluster Member
‖	Concatenation
K_i	Keys of the node i
D_i	Detector of the cluster i
EN_DATA(C_N)	Encrypted data of node C_N
R	Transmission Range
$CH_i \rightarrow CH_j$	Cluster head CH_i transmits the encrypted data to cluster head(next hop) CH_j
$CH_i \rightarrow BS$	Cluster head CH_i transmits the encrypted data to the base station BS_j
C_N->HELLO( )	C_N broadcast HELLO message in a transmission range R
$C_M \rightarrow C_N$:ACK()	C_M acknowledges to HELLO message sent by C_N
$BS \rightarrow C_N(EMBED(K_i)^n)$	Base station BS embeds n number of K_i keys into C_N, where n is a pre-defined value and remains constant for all sensors.
EN_DATA(C_N) $\rightarrow CH_i$	Cluster members C_N transmits the encrypted data to the cluster head CH_i
$CH_i \rightarrow$EN_DATA(C_N) ‖ EN_DATA(C_M) ‖ EN_DATA(C_P) ‖ EN_DATA(C_Q) ‖ EN_DATA(C_R) ‖ EN_DATA(CH_i)	Cluster head CH_i Concatenates its encrypted data with the encrypted data obtained from cluster member C_N, C_M, C_P, C_R, C_Q
$D_i \rightarrow CH_j$	Detector of the cluster i transmits the encrypted observed data to the next hop j

Table 1 : Notations used in the paper

IV. Flow chart and algorithm

A. *Algorithm*

Step 1: The base station generates n number of keys and embeds the keys into the sensors. Each sensor is given a unique ID which identifies itself and its ID can be utilized to authenticate itself.

Step 2: After deployment, the sensor broadcasts HELLO message after it gets activated. The sensors within the transmission range R, acknowledges the message by sending back HELLO message and identifying itself by the unique ID.

Step 3: The sensors authenticate each other and maintain a list of its cluster members.

Step 4: After the formation of cluster, the cluster members chooses one among them as its cluster head depending on the energy it possess, proximity and probability of number of times it is been nominated as the cluster head.

Step 5: The cluster head chooses a key randomly from its key pool, distributes the key along with the intensity the cluster members should utilize to transmit the data.

Step 6: The cluster members sense the data, encrypt it using encryption key and transmits the data to the cluster head. The cluster head in turn aggregates its data along with the cluster members and transmits the data to the next hop/base station.

Step 7: The base station analyzes the data obtained by the cluster head and the detector of cluster, does a comparative study and concludes whether a node is compromised or not.

Step 8: If a node is compromised, the base station broadcast the message to the network. In turn, the nodes communicating with the compromised node blacklists the node and stops future communication with it.

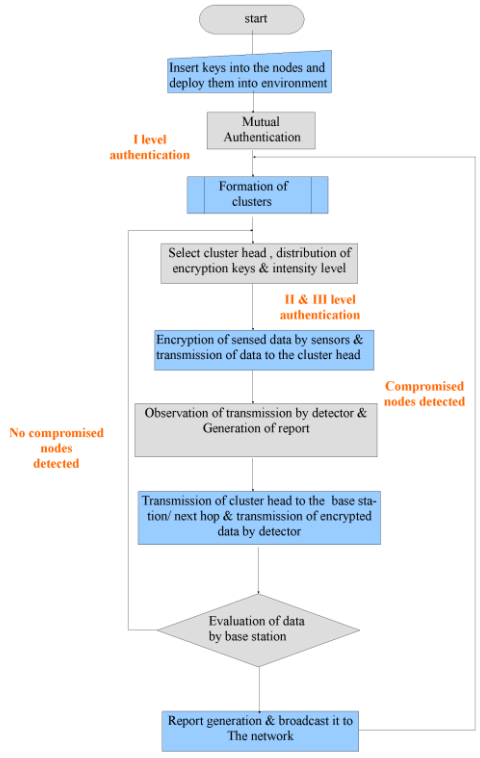

Fig 1 : Flowchart of TAWSN

V. ASSUMPTIONS

ASSUMPTIONS

The following assumptions are been made in this paper–

- The network is assumed to have 500 nodes utilized to monitor the environment. The nodes are dispersed either manually placed or dispersed using a helicopter. A cluster consists of 7 nodes including one cluster head and one detector. If deployment is done using a helicopter, the nodes which make up a cluster are dropped together. This gives a better option for the sensors to group themselves into a cluster. The nodes within a transmission range R, form a cluster.

- The nodes are assumed to be uncompromised till the formation of clusters. The behavior of the nodes changes if it is controlled by the intruder. The usual tasks assigned to them are not accomplished on time/ not at all.

- The base station is assumed to be trust worthy. The keys are generated randomly by the base station and embedded inside the sensors memory. The keys embedded are mutually exclusive from each other. The base station stores individual cluster's data. A list is being maintained as which cluster sends what data.

- The base station is also responsible for doing comparative study between the readings sent by the detector and cluster head. After a detail study the base station, concludes whether any node in the network is under intruder attack or not. If yes, it broadcasts the information to the network as to which node is supposed to be blacklisted.

VI. TAWSN MODEL

A. System Architecture

Table 2. Energy consumed by epic mote during different stages of its lifespan

Mode	Energy consumed
ON MODE	19.7mA
Transmit	17.4mA
Read	7mA
Write/Erase	12mA
Radio sleep	1μA
Flash sleep	5,4μA

The paper utilizes EPIC mote to form a cluster. EPIC is circa 2008 open mote platform used form application driven. EPIC core including systems are used for home Energy tracking, solar-power environment monitoring, body worn activity sensing and mobile air quality sampling. The processor is 250 Kbit/s 2.4 GHz IEEE 802.15.4 Chip on Wireless Transceiver; Texas Instruments MSP430 microcontroller 10K of RAM and 48K of flash memory.

A standard configuration depicted by table 2 is being set before the deployment. The different modes of the mote signify what amount of energy is being utilized in different state of the node. A small variation in the intensity during transmission of data is made in this paper. The detector in each cluster analyses the intensities of each data being transmitted inside the cluster. Any variation in them leads to suspicion of legitimate nodes in the cluster. The adversary will be unaware of the arrangement of intensity made in the network and hence will concentrate to draw the traffic towards itself.

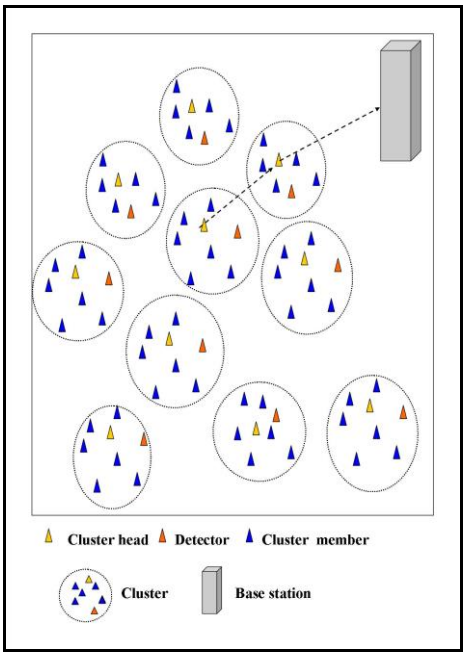

Fig2: Depicts the Network model where sensors are deployed for observation

A. Generating a random key pool

A key pool of n keys is generated. If the number of sensor nodes are r in number, then r*(r_k) are generated. Each node will be embedded with r_k encryption keys. If n is total number of keys, then K = {k1, k_2, k_3…k_n} is the key pool

being generated. The more the numbers of keys are embedded, the more would be the security to protect data. Care is taken to check, that the keys that are embedded in each sensor node are mutually exclusive to each other.

$$BS \rightarrow C_N(EMBED(K_i)^n)$$

B. Deploying nodes and formation of cluster

The nodes are embedded with keys before deployment. The nodes and base station share the master key. After the nodes, are being deployed they broadcast HELLO messages. The nodes within a certain range send the reply to form the cluster. After the formation of the cluster, the cluster head is chosen depending on energy level it contains. The information about the cluster head chosen along with its cluster members is sent to the base station.

$$C_N\text{->}HELLO(\ )$$

$$C_M \rightarrow C_N : ACK()$$

C. Choosing encryption key and intensity of data transmission

The cluster head randomly chooses a key and distributes the key to other cluster members. There comes a possibility that the mote may get compromised providing the entire data set stored in the mote. Once the adversary takes the control of the mote, it focuses on hindering data transmitted by other motes, modify the data to giving a different picture of the situation of the under surveillance. The adversary will not be able to maintain same intensity as it has to broadcast itself as the node nearest to the base station.

The adversary on the other hand will not be able to notice the intensity agreement between the cluster members. Hence maintaining the same intensity among all the transmitted data helps the detector to notice the compromised node quickly. The intensity of data transmission is decided by the cluster head and distributed to other cluster members. If the regular transmission intensity is I_i, then e is chosen such that $0.1 < e < 1.0$. Then the final intensity If is calculated by using equation (1).

$$\mathbf{I_f = I_i + e} \qquad \mathbf{(1)}$$

D. Transmitting the data from the cluster to the base station

The cluster member of the particular cluster transmits the encrypted data to the cluster head. The cluster head merges its encrypted data with the derived list and forwards it to the sink/next hop.

$$EN\_DATA(C_N) \rightarrow CH_i$$

$$CH_i \rightarrow EN\_DATA(C_N) \parallel EN\_DATA(C_M) \parallel EN\_DATA(C_P) \parallel EN\_DATA(C_Q) \parallel EN\_DATA(C_R) \parallel EN\_DATA(CH_i)$$

$$CH_i \rightarrow CH_j$$

$$CH_i \rightarrow BS$$

E. Detecting intruder

The mote that behaves like a detector in each cluster monitors all the activities of the nodes in the cluster. The intensity of the data transmitted is monitored by the cluster head at the time of receiving the sensed data and detector node. The detector node sends periodical reading about the activities of the cluster. The detector node behaves both as a detector monitoring the activities of the cluster and a normal node which senses the data, encrypts it using the encryption key and forwards it the cluster head. Behavior of the detector node as a normal node conceals the monitoring activity from the view of the adversary.

F. Security analysis

Report is generated utilizing the following scenarios:

1) Cluster member or the cluster head is a compromised node:

The base station chooses a node in a cluster as a detector node after authentication. The detector node behaves as detector and as a normal node sensing the environment and transmitting reading to the cluster head. The detector in each cluster monitors ongoing activities in each cluster and sends the periodical reading to the base station. After every cycle, new detector is allocated to the cluster (based on its previous behavior in the cluster). Since the detector behaves as a normal node providing reading to the base station, the adversary will not be able to distinguish between the normal node and the detector.

After obtaining the information about the compromised node by the cluster head or detector of the cluster, the base station broadcasts the information to other nodes in the network. In turn the other nodes, black list the compromised node.

2) Cluster head is compromised

If the cluster head is compromised, another cluster head is assigned the job to aggregate the data and forward it to the base station. A new encryption key is randomly chosen by the newly appointed cluster head and distributed to other cluster members after authentication.

If one of the cluster members is compromised, then the existing cluster head chooses another encryption key, authenticates the other members and distributes the key to all the cluster members.

3) Detector node is a compromised node

The base station sets the time at which it has to receive periodical readings from the appointed detector node. If the node is compromised, it has a large probability of not sending the readings on time. Based on this, base station instructs cluster head to authenticate the detector node and based on the report generated by the cluster head, base station concludes whether the detector is compromised or not.

The adversary will not be able to track the detector node as monitor node, due to the regular activity of the detector node. On such circumstance, the adversary having the control of the detector node will not be able to send periodical reading. Under this circumstance, the base station instructs the cluster head to authenticate the detector node.

Based on the reply of the cluster head, the base station employ's another cluster member as a detector node. The cluster head chooses another encryption key and distributes to the other cluster members.

VII. Simulated results

The work is been simulated using NS2. The dimension of the network would be 500m*500m. The sensors are distributed uniformly in the network. 500 nodes are deployed in the network uniformly.

After deployment the cluster are formed (assuming none of the nodes are compromised). In this paper, the cluster consists of 6/7 nodes in its cluster. 32 clusters have 6 nodes each and 44 nodes have 7 nodes each. A cluster has 1 detector, the cluster head is chosen depending on the energy it possess, proximity from the base station/ next hop and probability that the node has been assigned as the cluster head.

The length of the encryption key used is 132 bits + length of intensity is 4 bits, totally 136 bits is been transmitted to the cluster members by the cluster head. Utilizing this data, the cluster members encrypt the sensed data and set the intensity to transmit the encrypted data to the cluster head. The cluster head accumulates all the data and transmits the encrypted data to the next hop/base station.

A. Energy consumption

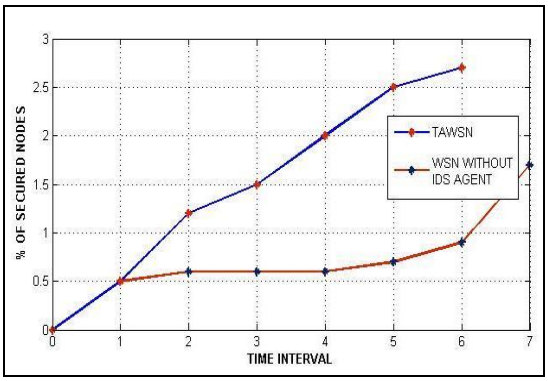

Fig 3: Energy consumption

Energy is an important resource for the nodes. As these nodes are deployed in unattended areas, they cannot be recharged. As the process advances, nodes will be spending major amount of energy on transmitting data from one node to another. Sensing the environment and encrypting the sensed data consumes least amount of energy.

Hence in this paper, clusters are formed which balance the network's energy. A cluster contains 6-7 nodes as its cluster members. One of the cluster members is assigned as the detector (which acts as a normal node, sensing environment. Apart from this activity its task is to observe other cluster members and provide periodical reading to the base station). Assigning a detector in the cluster conserves energy to certain extent. If one of the cluster members is compromised, the detector will be able to catch it in act and notify the base station. The base station in turn can warn other nodes in the network about the malicious behavior of the compromised node.

The cluster head is chosen depending on the amount of energy the nodes possess, proximity ratio and probability it is been nominated as the cluster head. Utilizing this method, equal opportunity is given to all the cluster members satisfying the above constraint.

Adding additional security where each cluster maintains its own transmission intensity may increase energy to certain extent, but the technique adopted secures the system from compromised nodes (the nodes under control of intruder can drain energy in the network, the compromised nodes can forward false values to next hop/base station consuming the energy of itself and other nodes which forward its packet.)

Hence the energy to be used is being distributed between all the sensors. The paper adopts a method where the cluster head is chosen depending on energy it possesses at the same time security is also addressed. Simulated results as in fig 5 show that there is an increase of 30% of energy consumption compared to the approach.

B. *Sybil attack*

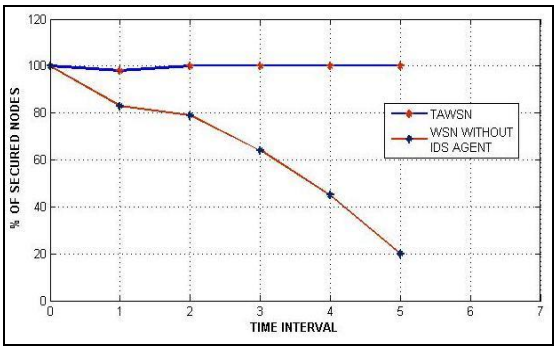

Fig 4: Result of Sybil Attack

A Sybil attack is one in which an attacker subverts the reputation system of a peer-to-peer network by creating a large number of pseudonymous entities, using them to gain a disproportionately large influence. A reputation system's vulnerability to a Sybil attack depends on how cheaply identities can be generated, the degree to which the reputation system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and whether the reputation system treats all entities identically.

The authentication takes place between the cluster members before the formation of cluster. After this authentication, there is a possibility of the network getting intruded by the adversary. The intruder can take control of some nodes, steal the information from them, can create multiple identities, and dispatch false information to the base station. These compromised nodes are not only draining the energy of the network (energy of itself + energy spent by other nodes to forward the data to the base station), the integrity of data is reduced.

This paper takes care of these situations and takes precautions by authentication of cluster members as its first initiative. Encryption Key is being distributed to add additional security for the data being transmitted from one end to another. Third layer security is added, by adjusting the transmission intensity of all the nodes in the cluster to standard communication intensity for that session. This provides enhanced security to the cluster.

Simulated result as represented in fig 2, show that the percentage of secured nodes is increased by 34% against Sybil attack.

C. *Wormhole attack*

Wormhole attack is where the attackers records the data at one location in the network, tunnels them to another location and retransmit the data to the network. This kind of attack, can repeat the telecast of the data from a different location. This provides false illusion to the base station (integrity of the network is at stake). Sending the same data repeatedly hides the actual situation of the network from the base station.

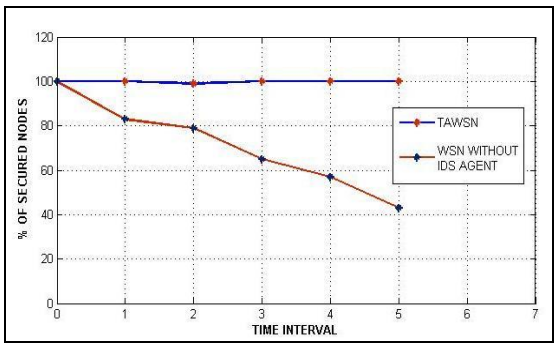

Fig 5: Result of Wormhole attack

This paper adopts a protocol where cluster head for a particular session chooses a key randomly from its key pool and in addition to the intensity of the data to be transmitted is chosen by the cluster head and information is being dispatched to the cluster members. A detector in the cluster keeps continuous watch on the cluster members and sends periodical observation report to the base station. Providing three levels of security assures the integrity to the network from wormhole attack.

The defense against wormhole attack is increased by 27.8% utilizing this approach. Fig 3 shows the representation of the simulated results.

D. *Sinkhole attack*

Description	Quantity
Dimension of the network	500m * 500 m
Total number of nodes in network	500
Distribution of nodes	Uniform
Number of detector nodes	1 detector per cluster
Total Length of encryption key	132 bits
Length of intensity	4 bits
Number of cluster members in the cluster	(6 nodes*32 clusters) + (7 nodes * 44 clusters)
Number of keys stored in nodes	75
Number of clusters in the network	(32 + 44)= 76 clusters
Total number of keys in the cluster	75^n, where n is number of cluster members

Probability values	TAWSN
Probability of detection of compromised nodes	>=0.8
Probability of false alarm	<=0.89
Probability of data integrity	>=0.88
Probability of reliable data reaching base station	>=0.9

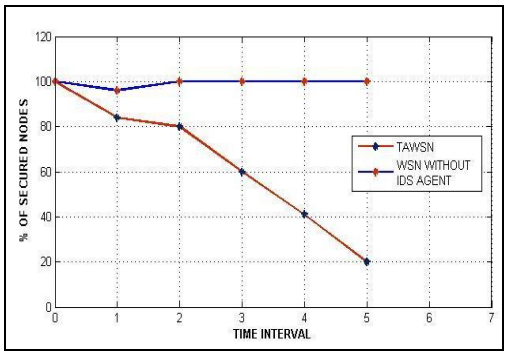

Fig 6: Result of Sinkhole attack

Sinkhole attack is where a malicious node can be made very attractive to the surrounding nodes. The node can broadcast (convincing that it is the next best node to closest to the base station). The neighboring nodes can get swayed away by this and hence the compromised node will gain trust of its neighboring node. When a node becomes a sinkhole, it becomes the hub for its vicinity and starts receiving all the packets going to the base station.

The node under sinkhole attack draws the data of all the neighboring nodes may modify/deny sending the data. This attack hence descends the integrity of data reaching the base station. Simulating the work increases the security to the data by 29.8% against sinkhole attack.

Table 3. Implementation details

Table 4 Simulated result

VIII. Conclusion

In this paper authentication of data and integrity of data is given higher preference. Authentication is a process, where identification of the two-parties is verified for future secured communication. In this paper authentication is done before the cluster is being formed (assuming that nodes are not compromised). The list of cluster members which whom they are imparting data is being maintained in their memory.

Integrity is a process, where the data sent by the sender remains unaltered till it reaches the authorized receiver. In this paper, encryption is being implemented to preserve integrity of the network. The encryption key is being chosen by the cluster head randomly.

References

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," in *IEEE Communications Magazine*, pp. 102–114, Aug. 2002.

[2] L.B. Ruiz, L.H.A. Correia, L.F.M. Vieira, D.F. Macedo, E.F. Nakamura, C.M.S. Figueiredo, M.A.M. Vieira, E.H.B. Maia, D. Câmara, A.A.F. Loureiro, J.M.S. Nogueira, D.C. da Silva Jr., and A.O. Fernandes, "Architectures for wireless sensor networks (In Portuguese)," in *Proceedings of the 22nd Brazilian Symposium on Computer Networks (SBRC'04)*, Gramado, Brazil, pp. 167–218, May 2004.

[3] C.Y. Chong and S.P. Kumar, "Sensor networks: Evolution, opportunities, and challenges," in *IEEE Proceedings*, pp. 1247–1254, Aug. 2003.

[4] M. Haenggi, "Opportunities and Challenges in Wireless Sensor Networks," in *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, M. Ilyas and I. Mahgoub, eds., Boca Raton, FL, pp. 1.1–1.14, CRC Press, 2004.

[5] A.P. Kosoresow and S.A. Hofmeyr, "Intrusion Detection via System Call Traces," *IEEE Software*, vol. 14, no. 5, pp. 35-42, 1997.

[6] K. Jain and R. Sekar, "User-Level Infrastructure for System Call Interposition: A Platform for Intrusion Detection and Confinement," *Proc. Network and Distributed Systems Security Symp.*, 2000.

[7] T. Garfinkel, "Traps and Pitfalls: Practical Problems in System Call Interposition Based Security Tools," *Proc. Network and Distributed Systems Security Symp*., Feb. 2003.

[8] Y. Chee, J. Rabaey, and A. Niknejad, "A class A/B low power amplifier for Wireless sensor networks," in the Proceedings of the 2004 International Symposium on Circuits and Systems, vol. 4, 2004, pp. 409–412.

[9] Gauis, "Things to Do in Ciscoland When You're Dead," Jan. 2000, http://www.phrack.org/phrack/56/p56-0x0a.org/phrack/56/ p56-0x0a.

[10] Yu-Xi Lim, Tim Schmoyer,, John Levine, and Henry *L.* Owen," Wireless Intrusion Detection and Response" , Proceedings of the IEEE, *Workshop on Information Assurance United States Military Academy*, West Point. NY, pp. 65-72, June 2003.

[11] M. Tamer Refaei, Yanxia Rong, Luiz A. DaSilva, Hyeong-Ah Choi ,"Detecting Node Misbehavior in Ad hoc Networks", *ICC 2007 proceedings, pp. 3425- 3430, 2007.*

[12] D. Taylor, "Using a Compromised Router to Capture Network Traffic," unpublished technical report, July 2002, http://www.netsys.com/library/papers/GRE_sniffing.PDF.

[13] QiWang, ShuWang, ZhonglouMeng, "Applying an Intrusion Detection Algorithm to Wireless Sensor Networks", *Second International Workshop on Knowledge Discovery and Data Mining, IEEE* , pp. 284–287, 2009.

[14] Lei Li, Yan-hui Li, Dong-yang Fu, Wan Ming, "Intrusion Detection Model Based on Hierarchical Structure in Wireless Sensor Networks," icece, pp.2816-2819, 2010 International Conference on Electrical and Control Engineering, 2010.

[15] Chien-Chung Su; Ko-Ming Chang; Yau-Hwang Kuo; Mong-Fong Horng, "The new intrusion prevention and detection approaches for clustering-based sensor networks", *IEEE Wireless Communications and Networking Conference*, PP.1927 - 1932 ,Vol. 4 ,*DOI 10.1109/WCNC.2005.1424814*

[16] Wei-Tsung Su , Wei-Tsung Su, Wei-Tsung Su, "eHIP: An energy-efficient hybrid intrusion prohibition luster-based wireless sensor networks" ,The International Journal of Computer and Telecommunications Networking Volume 51 Issue 4, March, 2007 Pages 1151-1168 doi : 10.1016/j.comnet.2006.07.008 .

[17] Xiaojiang Du,, "Distributed detection of node replication sensor networks" *IEEE International Conference on Communications, 2008*, pages 1446 - 1450, doi :10.1109/ICC.2008.280.

[18] Hongbing Hu, Yu Chen, Wei-Shinn Ku, Zhou Su, Chung-Han J. Chen, "Weighted trust evaluation based malicious node detection for wireless sensor networks**",** International Journal of Information and Computer Security 2009 - Vol. 3, No.2 pp. 132 - 149, doi: 10.1504/IJICS.2009.028810.

[19] Qing Zhang, Ting Yu ,Peng Ning, "A Framework for Identifying Compromised Nodes in Wireless Sensor Networks**",** *ACM Transactions on Information and System Security*, Volume 11 Issue 3, March 2008, doi : 10.1145/1341731.1341733.

[20] C. Kidd et al. The aware home: A living laboratory for ubiquitous computing research. *In Proceedings of the Second International Workshop on Cooperative Buildings (CoBuild),* 1999.

[21] S. Intille., " Designing a home of the future", *IEEE Pervasive Computing,* 1(2):76–82, April 2002.

[22] L. Schwiebert, S. Gupta, and J.Weinmann, "Research challenges in wireless networks of biomedical sensors", *In Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking (MobiCom),* 2001.

[23] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J. Anderson, "Wireless sensor networks for habitat monitoring", *In Proceedings of the ACM International Workshop on Wireless Sensor Networks and Applications (WSNA),* 2002.

[24] D. Steere, A. Baptista, D. McNamee, C. Pu, and J. Walpole," Research challenges in environmental observation and forecasting systems", *In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom),* 2000.