International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 07 | July-2018 www.irjet.net p-ISSN: 2395-0072

A NOVEL APPROACH FOR INTRUDER MAPPING BY ID BASED AGGREGATION SCHMEME IN WSN

Shradha.R.Mukka[1], Mallanagouda.Biradar[2]

[1] *4th Semester M.Tech Student, Department of Computer Network and Engineering, AIET College, Karnataka (India).*
[2]*Asst.Professor, Department of Computer Science and Engineering, AIET College, Karnataka (India)*

Abstract - *In this paper, we proposed the wireless sensor networking based system data exchange and data aggregation through the nodes plays the important roles in the process of data exchange and security management. The network will be adapted to the set of the node Ids for the purpose of the managing, updating the nodes identity. Many of the current data aggregation works has major drawbacks such as centralized approach and the security issue as they are vulnerable for the external attacks. The issues has to be deal and it has to adopted for the higher security level by making the id based aggregation by digital signature of nodes in every simulation system in clustered network. The system will allow the user to track the data exchange through the nodes BS(base station), CH(cluster head). In addition we have proposed the IDS(intrusion detection system) by adopting the attacker scenario in the process of data aggregation*.

Key Words: **IDS,CH,BS,DS,ENERGY**

1. INTRODUCTION

In the system of wireless sensor network[1] where the end system of the users are always in the need of the data to be aggregated which has been transmitted or stored and some basic servers(in our case BS, CH). The need of the data is high as it is used in the multiple scenarios. Consider for an example ,the user of the client will ask for the data he or she needed which is supposed to be transmitted to them in a fixed route. The system should have the copy of the data in case of the data delivery fails and also it should be able to process motile data to the user at multiple locations. Hence the problem of data aggregation raises as the multiple copies for resends are n the nodes, which are once again needed to be aggregated based on the Id. But in providing security a digital signature is generated for each nodes at each simulation.

The data transmission system is consists of set nodes ,having unique ID or DS[2](digital signature) which will have a total transmission size of the data in communication of the wireless networks. in general the specific routes are discovered during the route establishment phase (which is the client) and considering the data transmission in the end-to-end system it should not result in searching the data as data should be made available to the user by the service of the server.

As shown in the below figure the architecture of id based aggregation method by digital signature have the multiple modes of operation,

•The base station :- controls all nodes in whole network

•The Cluster node : Independent nodes

•Cluster head:- controls the nodes in cluster network

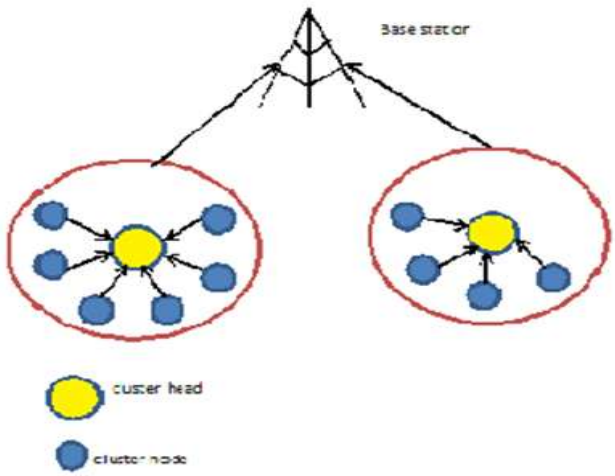

Fig.1- General Architecture

These are related to each other for the exchange of the information. The data is to be aggregated in the network and transmitted through the network. The general process for the proposed system can be listed as;

•The client/user sends the request for data

•Each data is allotted with the data id

•The server response to user by sending data

•Data is received at the user at fixed location

•User can verify data as requiredThese processed will be carried out in sequence will be explained in detail in the following subsections.

The main types of the data transmission are

•Centralized: which is unsafe and vulnerable for attacks

•Distributed : secured and efficient but in proposed work we didn't need to worry about the client as system acts as client and data is aggregated through the nodes based on the id.

1.1RELATED WORK

System requirement specifications (SRS) which gives information about the system behavior to be created. SRS includes both functional and non-functional requirements

- Functional Requirements

  Clients: an entity, it may be user or owner probably having a huge set of files is information to be saved on the cloud for data maintains and computation, can be either individual consumer or organization.

A. Owner

•Upload file

•Verify user

•send key

B. user

•request key

•verify file

•download file

Authority: a substance, with the skill & abilities that client does not possess, has authority to access as well as interpreting the danger to the user regarding cloud storage as and when requested.

•key request

•Owner details

•Consumer details

C. Cloud: a substance, with the capability to reserve a huge amount of user data and perform various operations on them.

•get key

•verify file

•partial decryption

D. Attacker: an entity, in which the unauthorized client not able to access the file or data. If any of the unauthorized clients try to modify file an alert message sent to the owner.

- Non Functional Requirements
  - Portability
  - Availability
  - Reliability
  - Efficiency
  - Cost

1.2 SYSTEM DESIGN

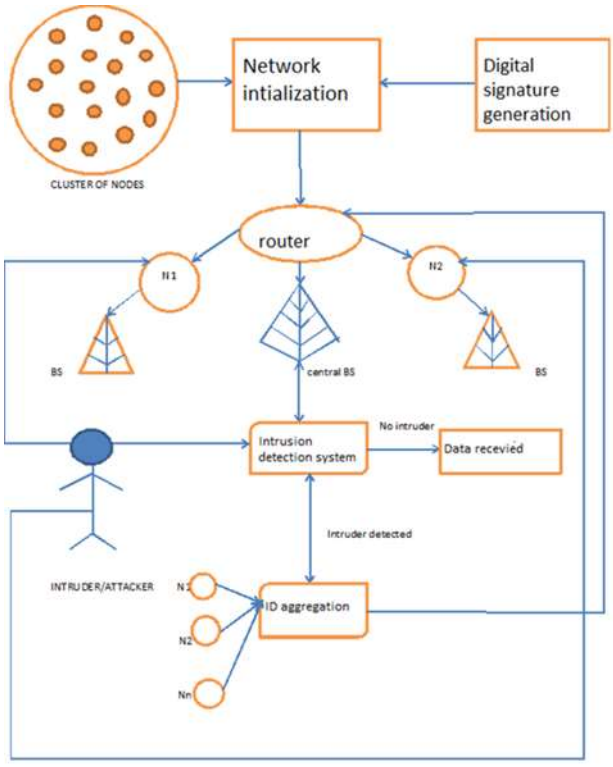

Figure 2: System design

WHERE, BS-BASE STATION, N1-NETWORK 1, N2-NETWORK 2

The above figure-2 depicts the System Architecture of the proposed system. Here initially the user has to choose a cluster of nodes which is initialized in the network initialization phase and each node generate there own digital signature in the digital signature module then the active nodes are feed into the router where the router divides the nodes into number of networks namely n1,n2 and so on and communication between network takes place through base station when there internal attack it is handled by the ids and if there is no attack the data is safely received.

2. IMPLEMENTATION DETAILES

2.1 modules

Proposed system contains two main modules –

1. Clustering Algorithm

2. Digital signature Scheme

1.Clustering Algorithm

Here model the wireless sensor networks. It is assumed that the nature of network is as follow:

•All of nodes are homogeneous .Each node has certain amount of initial energy E. Each node is assigned a unique identifier (ID).

•It consists of a BS, away from the nodes deployed in a square filed, through which the end user can access data from the sensor network.

Description of MWBCA (Multi-weight Based Clustering Algorithm)

All nodes should be alternately take turns to become CH, in order to prevent early death due to excessive energy expenditure. Nodes with higher residual energy should be selected as cluster-head than the nodes with low-energy. Or the CH election needs to consider following factors,

(1) Residual energy- Since the initial energy of each node is the same. If the node's residual energy is greater than it represent the energy consumed is less. So that node is more suitable is selected as the CH to balance the network energy consumption.

(2) Cluster head time count -Since all nodes have a responsibility to become as CH. Therefore, if CH has less time then it is more suitable to be selected as cluster head.

(3)The number of neighbors-Neighbor nodes are used to check amount of information transmitted and energy consumption.

2.Digital Signature Algorithm

It contains following steps –

1.Key Generation

2. Signature signing algorithm

3.Signature verification

1. Key Generation Sensor node creates a key pair, consisting of a private key integer dA, randomly selected in the interval [1, n-1] public key curve point QA = dA. G[8]

G – Elliptical curve base point, a generator of the elliptical curve with large prime order n.

n – Integer order of G

2. Signature signing algorithm Given message M, Digital signature is created by sensor node[9].

3. Signature verification At CH digital signature is verified If signature is valid then only message will get accepted otherwise rejected[10].

2.2.Experimental results

This section shows the screenshots of results

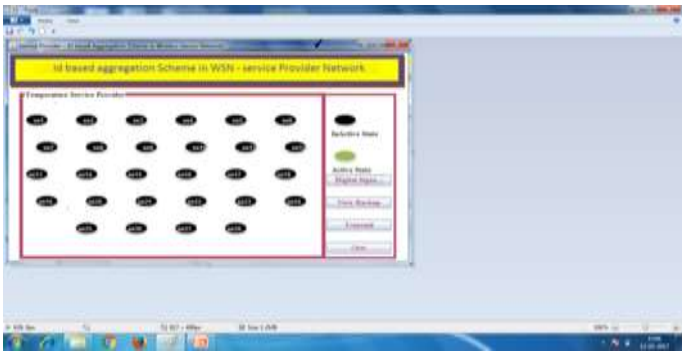

FIG 3: Node initialization active or inactive.

In this stage the user is allowed to initialize the system by generating the digital signature for each of the nodes in the system where the nodes are in either active or inactive state where inactive state are in black shade and active state are green shade.

FIG 4:Link establishment and routing in system

In this we can see the terminals of the proposed system. The service provider, router, base station and the ids manager. The work of terminals are illustrated in the following.

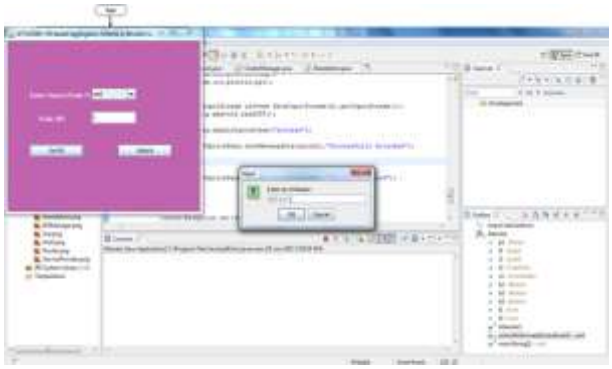

Fig.5 Attacker message

In the above figure the attacker scenario has been presented. In this scenario attacker attacks on the node by the Specific IP address and attacked. The attackers details re maintained in the system which can be used for the later use.

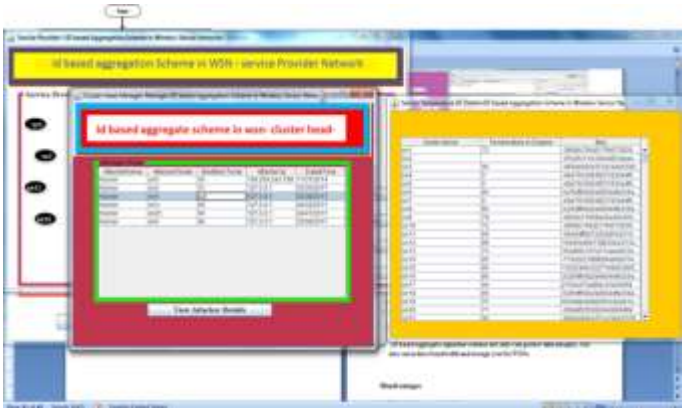

Fig 6 Attackers and sensor values of the id of the system .

In this we can see the CH maintaining the history regarding the multiple attacks on the proposed work by the external attacker. The attacker details like IP address, time date are stored. The attacker attacks on the energy value set as 0 are shown in our example.

Fig 7 Base station rectifying the energy status and verify the packets .

When the attacker is detected in the system the IDS will be active and it will detect the attacked nodes, which are marked in the red. These nodes are verified and the original value of the energy is restored to the nodes by IDS under the BS command.

GRAPHICAL REPRENTATION

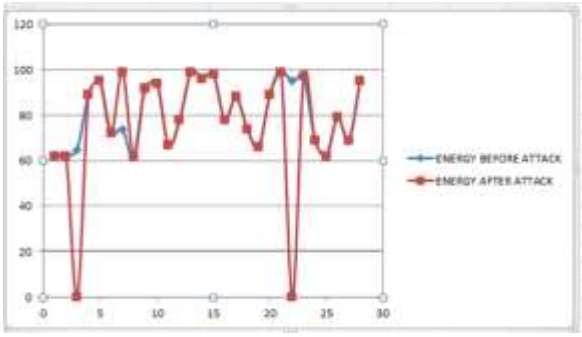

FIG 8:nodes vs energy

In this we can see the graphical comparison of the nodes energy level before and after attack of intruder. We can observe the system will be able to detect the attacker based on the node behavior and perform the Id based aggregating on the attacked node to achieve the security by re allotting the required energy. By this continuous effort the system will be able to solve the attacks by using the IDS to achieve the security and efficiency.

3. CONCLUSIONS

ID based aggregation schemes by the digital signature based authenticity has been a new concept I data exchange. higher level security has been achieved in the WSN with distributed environment. In addition the IDS detects and resolves the external attacker. The BS and the CH are nodes perform and controls the data exchange and information exchange. The attacker module has been introduces to see the system vulnerability.

REFERENCES

[1] Akyildiz, W Su, Y Sankarasubramaniam, E Cayirci - Computer networks, 2002 – Elsevier

[2] Katz, Jonathan "digital signature",2002-springer

[3] Huang Lu, Jie Li, and Mohsen Guizani, "Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks" IEEE Trans. Parallel &Distributed Systems,vol. 25, no. 3, March 2015

[4] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Comm. Surveys & Tutorials, vol. 8, no. 2, pp. 2-23, Second Quarter 2009.

[5] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660-670, Oct. 2008.

[6] A.Manjeshwar, Q.-A. Zeng, and D.P. Agrawal, "An Analytical Model for Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol," IEEE Trans. Parallel &Distributed Systems, vol. 13, no. 12, pp. 1290-1302, Dec. 2008.

[7] L.B. Oliveira et al., "SecLEACH-On the Security of Clustered Sensor Networks," Signal Processing, vol. 87, pp. 2882-2895, 2011.

[8] P. Banerjee, D. Jacobson, and S. Lahiri, "Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks," Proc. IEEE Sixth Int'l Symp.Network Computing and Applications (NCA), pp. 145-152, 2011.

[9] K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," Proc. Fourth Int'l Conf. Wireless Comm., Networking and Mobile Computing (WiCOM), pp. 1-5, 2012.

[10] W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Trans. Information Theory, vol. IT-22, no. 6, pp. 644-654, Nov.2005.

[11] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," Proc. Advances in Cryptology (CRYPTO), pp. 47-53, 2004.

[12] D.W. Carman, "New Directions in Sensor Network Key Management," Int'l J. Distributed Sensor Networks, vol. 1, pp. 3-15, 2005.