International Journal of Engineering & Technology, 7 (2.8) (2018) 477-487

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Authentication and overhearing to prevent internal and external attacks in WSN

Siri Maidhili R*, Karthik GM

Department of Information Technology, SRM engineering college, Kattankulathur, Chennai, India
**Corresponding Author Email: rsreemythili@gmail.com*

Abstract

Wireless Sensor Networks are usually the assortation of sensors, which are versatile in sensing the data based on multihued exertions. The cardinal bulge with the sensor networks is its dispersed nature. Since they are spread over, they sense and forward data from their dispersed areas. They consume high energy resources and vulnerable to various attacks. To prevail this bulge, source identity (signature) based authentication scheme is proposed on ECC to prevent external attacks and a neighbor monitoring scheme is proposed by overhearing to prevent internal attacks. Now the cardinal strike with the sensor networks are its bounded energy resources, they have a very limited / less energy resources, they cannot have a hefty application assignment. To prevail this strike and to improve the energy efficiency, a low energy consumption MAC protocol is acquainted called the IEEE 802.15.4 / ZigBee standards un the MAC layer, through which the data forwarding among the networks devours very low energy when compared to all other traditional methods. The main objective of the proposed work is to perform broadcast after authentication, to prevent resource consuming attacks through authentication externally and to construct a monitoring table for each node by overhearing and detecting them based on their activities if they are malicious to provide internal security to the network. The proposed work attains a minimal energy wastage along with security integrated in WSN communication. The ratio of efficiency comparisons of the broadcasting authentication scheme and monitoring scheme for the traditional and the proposed works for the factors secure authentication / monitoring and energy consumption is resulted to be as 7:2. Thus the proposed system has a higher endorsed based on the generated results.

Keywords: *Wireless Sensor Networks, Broadcast authentication scheme, elliptical Curve Cryptography, overhearing, External attacks, Internal attacks, ZigBee Communication.*

1. Introduction

Wireless Sensor Networks[WSNs]: Since WSN are largely accountable for data transactions, the energy resources should be imperative [1]. WSN largely involves an assemblage of sensors, that collaboratively supervises the applications which can involves whether temperate monitoring [2], embedded in microcontroller, health care [3], industries Business [4], Military usage, climate control, Incident emergency response, Earthquake monitoring, Sports [5] etc. The WSN are assorted with numerous sensors with the ability of sensing entrenched together and the nodes are breaking down with prismatic components like processing unit, storage unit, GPRS, Transceiver and the power pack. The Transceiver Utilities Radio frequency for the medium of transmission, the Controller is responsible for functionalities inside the sensors are controlled like performing the tasks data processing etc., Memory to store the collected data, The Power pack in the sensors are the challenging to replace. Thus, a battery should be inbuilt, that stays for a period of extension, Sensors are tiny devices, which only utilizes minimal energy which can range to 1.2-3.7 Volts [6].

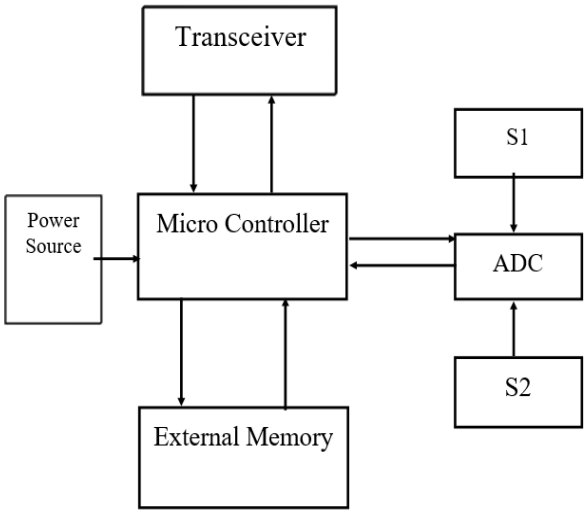


Fig. 1: Architecture of a Sensor Node

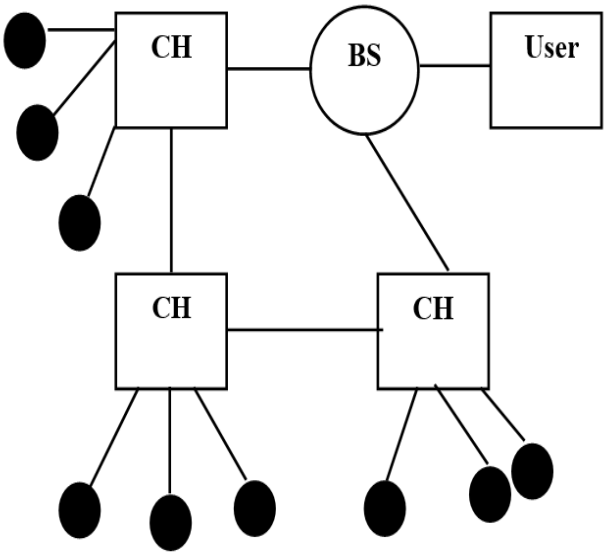


Fig. 2: Wireless Sensor Network

The sensor nodes gather the data from the dispersed areas based on the application. The cluster head(CH) aggregates the gathered data from sensor nodes(SNs) and forwards it to the Base station(BS). Now the BS receives the aggregated data and provides it to the end user. The architecture of WSNs is also about joining together and providing a remote network for both wired and wireless communications for propagating nodes. The WSNs is set up in such a way that a sensor node is comraded with a higher cubage resourced node is comraded with a higher cubage resourced node to act as a gateway to the neighbor node. Since they are dispersed in nature not all the CHs are connected to the BS. Thus, the SN collected data is acquired by the CH and is forwarded to the next relaying node to reach the BS. Thus, communication can occur based on the multi hops. The main challenges are the energy efficiency, Privacy and security [7].

Impersonation Attack: As discussed WSNs are utilized for various purpose like tracking and monitoring, irrespective of the purpose of usage or the application, the representation and persistence of security is cardinal. When compared to the wired networks, Wireless networks are highly vulnerable and exposed towards numerous attacks. This is because of the reason that the transmission medium of WSNs are radio frequency signals. The communication between them happens is like a broadcast mechanism since it transmits signals [8]. If a source wants to reach out the destination the source broadcasts, while the signals reach all the nearby neighbor which a threat can be. If an attacker stays in the network range, when the broadcasted signals can be received which can lead to attacks like node capturing attack, bogus packet injection attack, etc. Thus, making a secured transaction of data in WSNs is really challenging and important. In WSNs during the multichip data packet forwarding which involves various rely nodes in the transaction, the adversaries of the malicious node can easily rob the data packets, since it is all the signal broadcasting mechanism that works during data forwarding. Apart from stealing the data packets which works by the concept overhearing (each node can investigate the transaction of their neighbors since it again broadcasts mechanism) and controlling the packets because the captured packets contains all the details which includes the Source, Destination and their node ID's. In this way the attacker node can capture the packets during the data transmission and fake control over them [9].

Impersonation attack is all about a malicious node, hiding its identity and acting as a legitimate node, by altering its details with a legitimate node. An example scenario about impersonation attack is as follows:

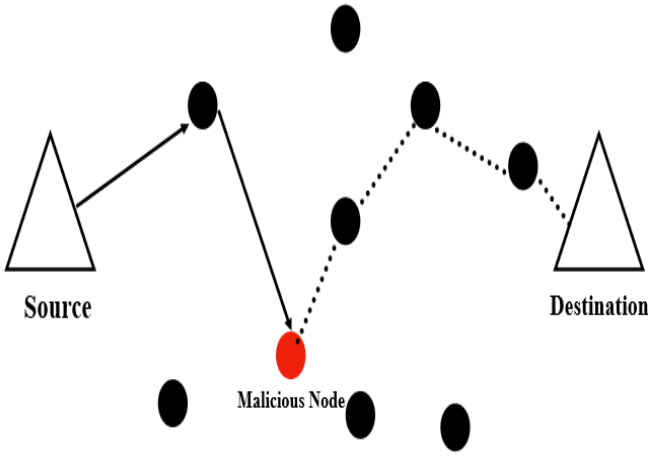


Fig. 3: Impersonation Attack

When a source needs to forward packet to the destination that happens through broadcasting mechanism. When the path goes from source to legitimate node followed by the legitimate node to the malicious node, the malicious node hides its identity and acts as a destination and receives the packet and does not forward/route it to the destination. This way it illegally acquires the data packet changing its original identity [10].

Authentication: Authentication can typically be defined as a procedure to validate the genuineness. The basic or the fundamental way of the authentication was like, Consider Server and user where user wants some confidential information (whose integrity cannot put on risk) the server immediately asks for an identification (if the user is genuine), Once the user sends the identity (which can be ID, password, etc.) the servers verifies if the identity is matched/validated the confidential information based on the request forwarded to the user, else the request is discarded. But in the traditional methods, there occurred man in the middle attacks(MITMS) during the transaction of validating the user identity. To overcome the above issue, the encryption and decryption with various were used which reduced the MITM attacks based on the authentication scheme complexity [11].

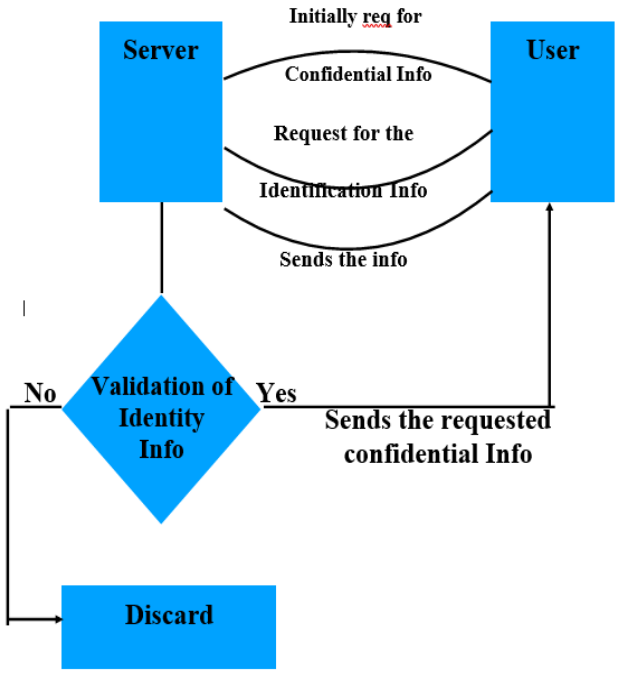


Fig. 4: An overview of Broadcast Authentication Scheme

Initially TESLA was the cryptographic scheme introduced that falls into the symmetric key cryptography which has acquired the user authentication data integrity utilizing the one-way hash method, Sender and receiver loose time synchronization message authentication code(MAC) and the detente secret key revelation which reduces the communication overhead and provides efficiency. Out of everything, it was stated by the µTESLA follower that they face severe active attacks due to the detente secret key and the MAC revelation [12]. The public key can give a solution to the above stated issues since it comes with adaptable working like there will be no need of key sharing initially for both distribution wise and pair wise. This was proven by a very limited resource usage in WSNs [13]. During the authentication of the public key infrastructure which states that the public key certificated is used which is a combination of the public key and user/ID certificates for the authentication purpose which again results in heavy energy consumption if it is implemented in WSNs [14]. Thus, an ID base (signature) was proposed for a light weighted authentication. Even this resulted to be expensive since it uses an expensive bilinear pairing [15].

ECC: In general, a standard sensor node can be assigned with a storage of 48kb of flash and 10kb of RAM which implies that the storage of private keys for each node is attainable but when it comes to the storage of public keys for each node is attainable but when it comes to the storage of public keys in the memory, it results to be unattainable. ECC attempts to provide a decent and a minimal sized key which provide the security at the same level as others [RSA, enTTS, NTRU] also with minimal processing time requirements and communicational overhead. ECC assigned with the 160-bit keys equalizes to the power of 1024-bit keys of RSA [16]. The below mentioned table shows the time taken by each encryption algorithm in the simulation results and the key sizes for a platform with 8 bits at 32 MHZ with a security level of 80 bits which again proves that ECC is efficient and better when compared, notably when implementing for WSNs:

Table 1: ECC Table

Asymmetric Algorithms	Time Taken for sign	Time Taken to Verify	Size of Public Key	Size of Public Key	Size of Private Key
enTTS (s,20,28)	17.75	181.5	52	49608	4591
ECC	203	203	40	20	20
RSA-1024	21748	108	128	128	128
NTRU_251-127-31	143	–	147	147	294

For the above-mentioned table précised finding results saying that ECC has the finest poise in terms of fastness, storage requisites, charge for communicational transactions, resource consumptions among WSNs [17].

Energy Consumption: The raising of WSNs are the composition of low radio technology and the advancement of microelectronics. This attribution leads to the enhancement of WSNs. In the blueprint of the wireless sensors construction, the lowest resource usage is to be considerable as a cardinal factor. They cannot transmit data that utilizes high resources since it is quite challenging to change or recharge the batteries [18]. There were also few mechanisms for productive scheduling developed for high sustainability of sensor networks like the sensors are set into sleeping time where they have no work assigned or if the assigned work is done by the sensors to save energy and few [19] also analyzed various routing algorithms to achieve energy efficiency. The cardinal feature that as to be taken into consideration during the design of sensor network is the transmission power, else it may affect resource consumption that also impacts on the network performance. Then the solution for the reducing the transmission range which leads to the less transmission power usage during the forwarding of packets to the nearest neighbors. An issue again arose declaring that when the transmission range is decreased, the probability of the successful transmissions also reduces and simultaneously the numbers of hops during the transmission increases which again leads to energy consumption since the time taken for transmission extends [20]. There standardized a technical framework by IEEE 802.15.4 which mainly focuses on minimal rated transmission in WSNs [LR-WPANNS – low rate wireless personal area network] was also acquainted which involves the configuration of physical layer. Next it contains a MAC layer that takes control of the physical channel access [21]. Upon the MAC layer consists of the convergence sub layer. This plays a role of providing the access to the higher layer i.e. the logical link layer of the standard IEEE 802.2. This architecture is also linked up with the upper layers to configure the network and for routing the data [22].

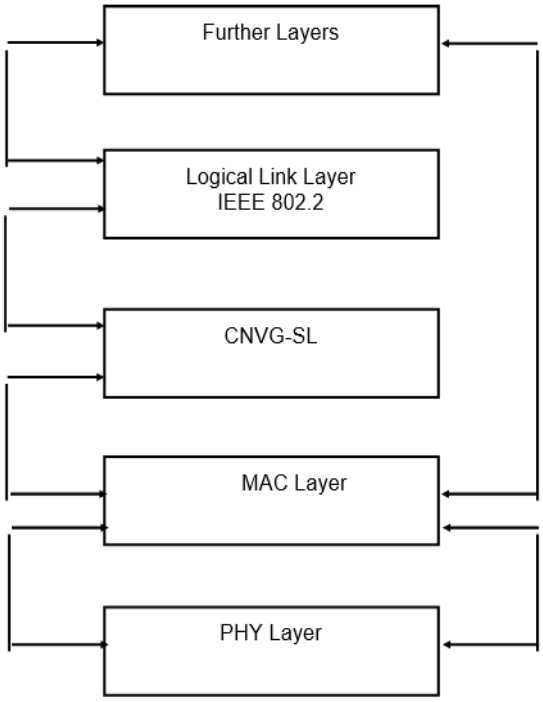


Fig. 5: LR-WPAN Architecture

ZigBee: ZigBee is the technology that is usually used for low powered networks as it is meant for its low power usage. The transmission range of ZigBee generally varies from 10m to 100m in the line of version and the topologies generally can be supported are star, tree, mesh topologies [23]. ZigBee is the most reasonable or even inexpensive technology that can be used when compared to other technologies such as Wi-Fi and Bluetooth. In conceptual transmission using ZigBee, the data rate is assumed to be 250kbps in 2.4 GHZ band. The basic ZigBee architecture can be represented as follows [24, 25]:

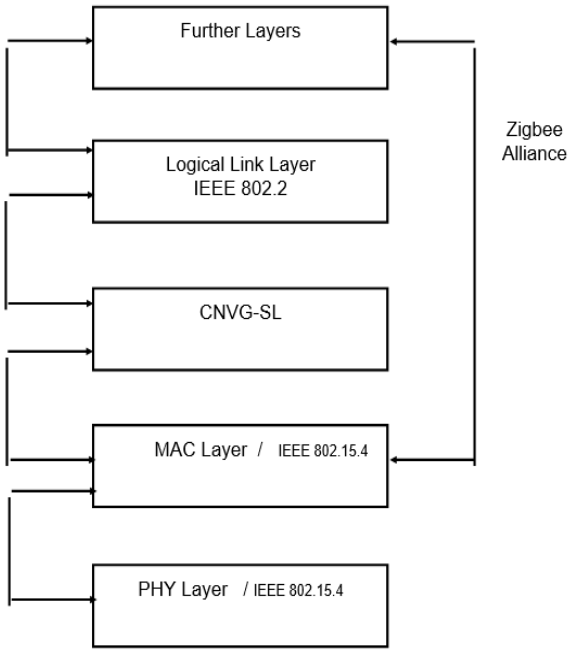


Fig. 6: ZigBee Architecture

Intrusion Detection System: Intrusion is grievous when it contrives the network. Thus, intrusion detection is cardinal to enhance and implement into any network. Since they also affect the CIA (Confidentiality, Integrity, Availability) [26]. IDS is generally classified into two types of systems (1) Network based IDS (2) Host Based IDS [27]. WSNs are generally classified as cluster of tiny sensors grouped together in a cluster of tiny sensors grouped together in a network, that can be utilized for various tracking and monitoring applications in which IDS should be bounded and should integrated in network [28]. In the network-based IDS intrusion detection system is set in the network which detects the intrusion network wise.

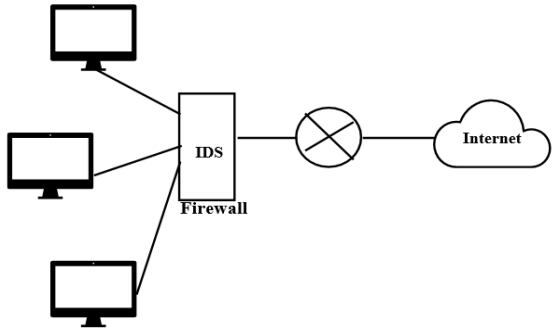


Fig. 7: Host Based Architecture

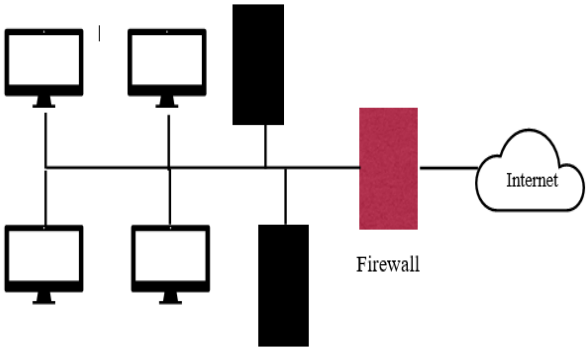


Fig. 8: Network Based Architecture

Overhearing: Since it is all the broadcast communication proceedings by nature of wireless sensor network, If the data transmitted by a node, all the other neighbor nodes who fall in the communication range in the network are liable to hear the broadcasted information. Thus, by hearing the neighbor nodes information, packet dropping attacks, reduction of delay during routing and increase the lifetime of the network can be achieved. The above hearing concept can also be stated as "overhearing" [29]. This overhearing handles the following challenges like (1) Detects if the node has too many messages in queue (prevents the dropping of packets) (2) Detects if the node instead of forwarding the collected data to the CH, forwards it to all the neighboring nodes (prevents the back-pressure messages) thus make sure to prevent unwanted bogus messages which provides network lifetime and sustainability [30]. Thus, due to broadcasting nature in WSNs, even if the neighbor is not in direct contact, all the other neighbor nodes will be able to investigate the transmitted data, if the nodes are in broadcasted network range. This type of technique provides transparency and prevents many insider attacks [31].

2. Related Work

WSNs are generally classified into cluster of tiny sensors grouped together in a network that can be utilized for various tracking and monitoring purposes. In WSNs clustering plays a vital role where there are many clustering techniques proposed to improve the network sustainability. Basically, a set of nodes are grouped together beyond their similarities and dissimilarities. Generally, information is gathered by the sensor nodes and is forwarded to the CH, where the CH aggregates the data collected based on many parameters like time stamp, distance between two nodes, etc. and sends only the aggregated data to the base station. This can improve the network lifetime, reduces time/ energy consumption, prevents data loss [32]

In WSNs, since all the messages are broadcasted, since the communication works based on the broadcasting procedure, authentication plays a dynamic role. Thus, the node authentication in a network is a mandatory to prevent external attacks. There were initially public key certificates for authentication purpose but still the certificates consumed storage which resulted to be costly during communication cost. Instead of the usage of public key certificates during transmission for authentication, ID based signature scheme was proposed which was pairing free also with a message recovery parameter to reduce the computational and communication cost [33].

Impersonation is all about hiding the original identity or pretending to be somebody. Impersonation attack in WSNs is malicious node hiding its identity and trying to pretend like a legitimate node to transmit confidential data, a confidential way of sharing method in a distributed way of data transfer is subjected. This was achieved by encrypting the data initially and transferring the data in a dispersed way in multi paths, so that even if the attacker overhears, only the partial data can be acquired with which a complete data stealing is not possible [34].

ECC as stated in the introduction is highly preferable since it is highly recommended for WSN. It uses minimal power for processing, it takes the minimal time to generate a signature, take a minimal time to verify the signature, it has the minimal signature size, public key size and private keys. This paper proposed three stages namely the (1) Initialization stage (2) Registration stage and finally the (3) authentication stage using Elliptical Curve Cryptography(ECC) for a secured data transmission in the sensor network [35].

In WSN authentication implementation is extremely cardinal. To establish a secured authentication scheme a secured two-way authentication scheme was proposed in this paper. There constructed a two levels of authentication mechanism, the user and requests to a server to join the network with a key allotted initially the server verifies and forwards it to the network, the network

again verifies and replies to the server only if the user is legitimate. Finally, the server grants the request of the user and allows the user to join the network. The user is then the part of the network and will be involved in the data transmission transactions of the network [36].

In WSN, false data injection attacks chances very often. It is important to detect the attack at the initial launching stage and minimize the occurrence of this attacks. In this paper a detection method was proposed by adapting a hierarchical Bayesian space time methodology which aggregates the attacks in the network using a divider difference filter. The above proposed network stands by to provide a good resistivity against false data injection. There were stages assigned for the false data injection attack (1) Initialization of cluster (2) Updating of state of network if any false data injection attack occurred (3) The counter measure update along with the calibration of state [37].

Since everything in WSNs work on the broadcasting nature, all the nodes that lie in the network transmission range will be able to hear each other. Thus, this means that all the neighbor nodes can overhear each other. Thus, this means that all the neighbor nodes can overhear each other when they lie in the transmission range, even if they are not directly connected or in line of contact with each other. This overhearing includes everything RTS/CTS, the request for the data to send and the actual data transmission when there is a clear path for the data to send even if the node is not either a source or a destination, but just a node that lies as an intermediate in the network broadcasting range [38].

In the WSNs, the energy resources consumption is a challenging issue that must be taken into considerations since they cannot sustain high transmission. They consume low energy all the time and moreover their batteries are rechargeable a replaceable. Thus, providing a low energy consumption factor is mandatory for the network to sustain. An analyzation is made from end to end transmission like how many packets reached from source to destination and how many packets were dropped. Based on the analysis, an energy saving scheme was framed based on the greedy approach [39].

WSNs works only with low power. ZigBee is the platform which when integrated with WSN results in low power consumption. All the nodes when using ZigBee for communication consumes very low power. The architecture set up is initially constructed with cluster nodes to cluster heads, cluster heads to super cluster head and then to the base station or the coordinator. The results for the energy consumption is as follows [40].

Table 2: Energy Consumption of Sensor Nodes

Type of Node	Energy consumed during Receiving	Energy consumed during Transmission	Energy consumed during Idle	Energy consumed during Sleep
Sensor node	0J/day	0.3873	0.0830	2.9231
Cluster Head	0.0792	1.9368	0.8300	2.8137
Base Station	0.0792	1.9368	0.8300	2.8137

3. Proposed Work

NS2: WSNs are usually the assortation of sensors, which are versatile in sensing the based on multi headed exertions. There are many topologies that can be constructed in WSNs from a simple kind of star network to a complex kind of multi hop mesh network. In WSNs comprises of sensors which are considered the tiny compact computers that can fetch the demanded data based on the application with a minimal computational and communicational cost.

To display the variations virtually, network simulator is used. Generally, a network simulator is defined as a thread kind of software which fetches out a virtual construction of node. Their behavior or any changes in the network can be viewed without a necessity of construction of actual network. NS2 provides the following features (1) The performance evaluation for the existing network. (2) Future prediction flow of network before construction. (3) Analyze results for large scale experiments without implementation [41].

4. Network Architecture

A WSN is set up based on a clustered network along with a simultaneously constructed hierarchical model which requires one or more hops to reach the base station and pass the collected and aggregated data. The network is setup in such a way that a cluster of nodes are in a dispersed manner based on the application requirements.

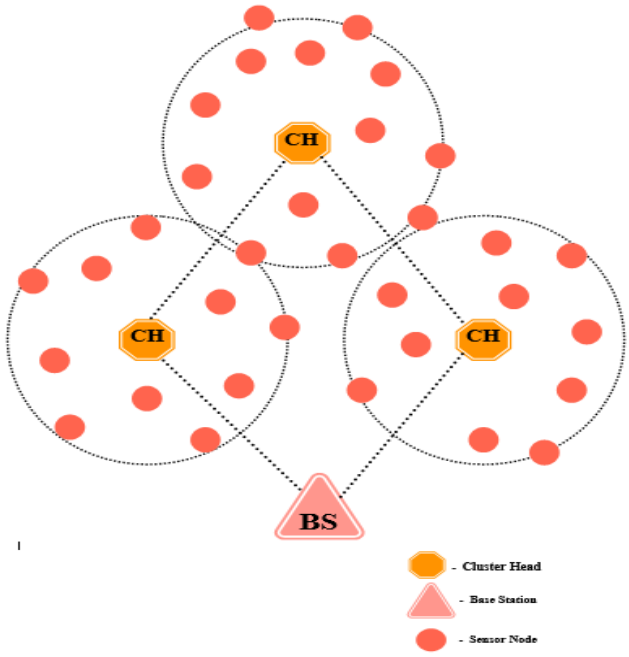


Fig. 9: Network Architecture of WSN

Now the sensor nodes are the nodes at the base/bottom level that senses and collects all the data and sends it to the CH. The CH now aggregates the data based on the time stamps, Distance between two sensors, etc. and forwards it to the one hop CH or directly to the base station based on the network design.

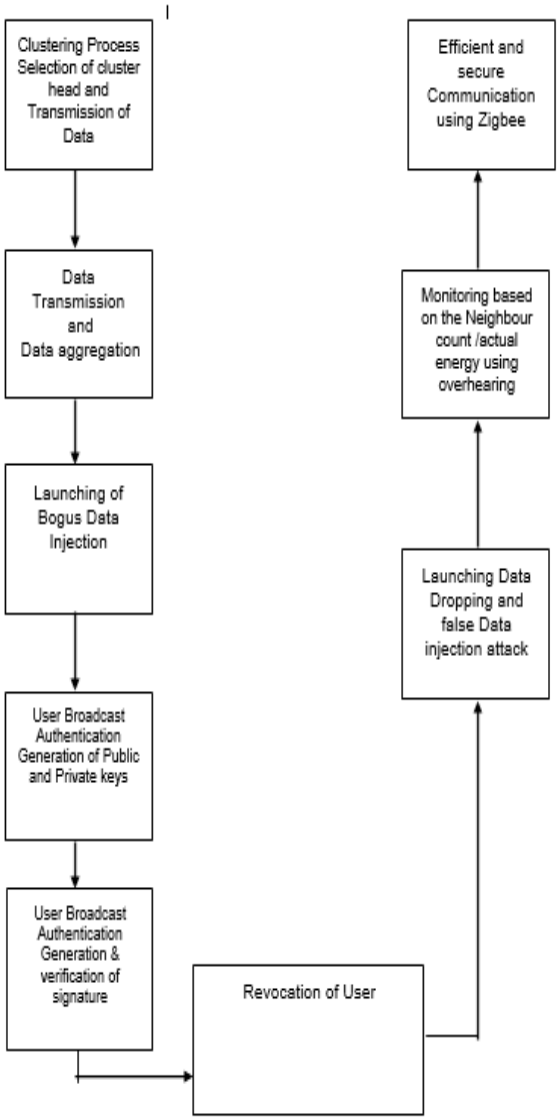


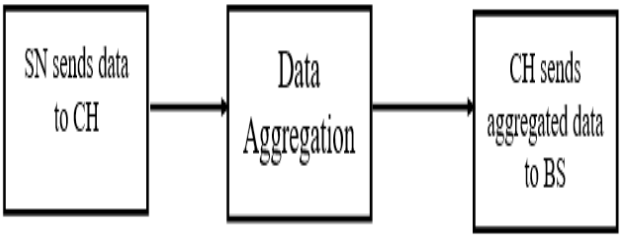
Fig. 10: Modules for the proposed Work

(1) Clustering Process: Selection of cluster head and transmission of data

Input: Sensors
Output: Formation of cluster & CH selection
WSN is all about broadcasting packets. Initially all the nodes that exist in the broadcasting range sends hello packets to each other. All the nodes receiving the broadcasting hello packets save their neighbor table for further communication. Likewise, a cluster is formed. Next comes the CH selection. Then the CH is selected based on high energy. The node becomes a candidate node if its neighbor count is greater than that of the threshold value.

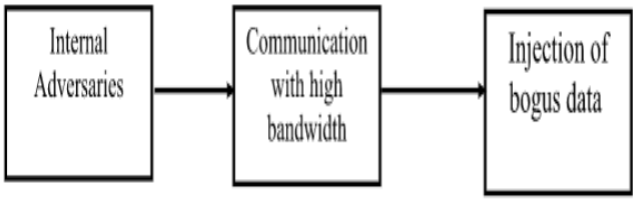
(2) Data transmission and Data Aggregation

Input: Collected data by SN
Output: Aggregation of data by CH
After the CH selection, the CH broadcasts the message to the network indicating the post of CH and all the SNs register entry in the table and consider that node as CH and the data forwarding is done. Before that there is a special authentication scheme for security issues.



(3) Launching Bogus Data Injection

Input: Packet broadcast
Output: Attacker launching bogus data packets.
In WSN there are many occurrences of malicious attacks since all the malicious nodes consists of adversaries. Generally, adversaries are classified in two categories, internal and external adversaries. The internal adversaries of malicious nodes consist of keying content of all legitimate nodes and have authentication because of that keying content and creates bogus packets in the network whereas the external adversaries do not have any content of the keying content. The keying content of the adversaries include all the details like energy of the nodes, etc. The adversaries are so significant that they can inject bogus packets with a very high bandwidth which results in the drain of energy levels of the legitimate nodes.



(4) User Broadcast Authentication: Generation of Public and Private Key

Input: Node ID
Output: Public key, Private Key
The sink node has a table of all the public keys. If a unknown user (30) wants to enter into the network, it initially gets the public key of the node that it wants to communicate (15), User (30) node generates an encrypted signature with its node ID and private key using the ECC encryption algorithm and sends a RREQ to the communication node (15). The node 15 fetches the public key of user 30 from the sink node and decrypts it is using ECC. If legitimate authentication is done. In the attacks scenario node (30), the attacker node pretends to be the legitimate user (40) steals the node ID, since it is globally available and encrypts it with its own (40) private key. Since it is confidential, now when sends RREQ to 15, the 15 tries to decrypt.it with public key of 40, but mismatches since the private key in the encrypted packed is of node 30 and not node 40. In that case the authentication failure occurs, and the node will be discarded to enter the network.

(5) User Broadcast authentication: Generation and Verification of Signature

Input: Valid Signature
Output: Signature validation
During the authentication process the source broadcasts the route request (RREQ) along with a signature (SIGN) to reach the destination (D) among the network. The RREQ consists of the sender information (node ID). The signature is generated by encrypting the node ID and the public key of the S by ECC.

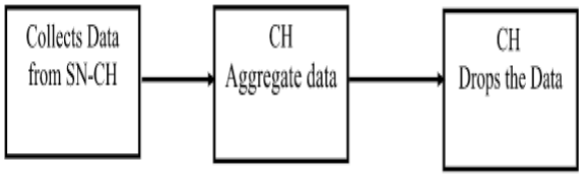
During broadcasting, the neighbor node that receives the RREQ initially decrypts the SIGN by the public key of S, based on the sensor information, if the signature gets validated it is considered as legitimate RREQ from S and authenticates each other, then forwards it to the next hop neighbor attaching its RREQ and SIGN also.

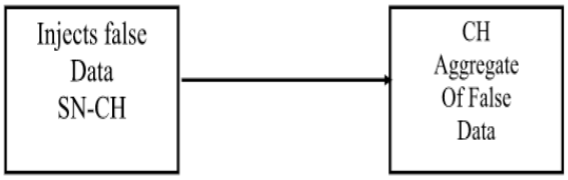
(6) Revocation of user

Input: Invalid Sign
Output: Invalidation signature
In the attacker scenario, if the attacker pretends to be a legitimate user and sends bogus broadcast messages, the attacker is dredged due to the mismatch that occurs while the signature is verified. If the sign mismatches during the decryption process, the RREQ from S is malicious and that RREQ will be discarded which can prevent impersonation attack and flooding attack. Thus, based on the RREQ and SIGN the secure authentication takes place. Finally, when it reaches the destination, the request reply (RREQ) is send to source by backtracking the path. This way any attacks, that can occur externally from nodes can be prevented.

(7) Launching Data Dropping and false data injection

Input: Transmission of Data
Output: Data Dropping attack and False Data injection.
In the network a node manipulates the other nodes telling that it has the shortest path and acquires all the data which is referred to as black hole attack, the CH declares a shortest way and acquires all the data from the sensor node, discards it or utilizes it based on the motive without forwarding it to the destination [44].

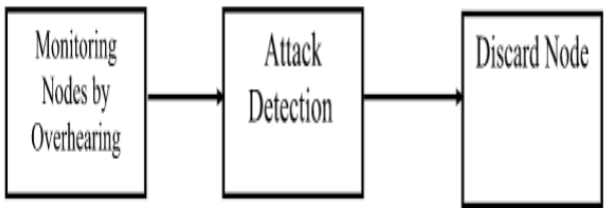




False data injection is all about injecting false data into the network. If it is CH, the CH collects all the data from the SN but sends false data to the BS [45].

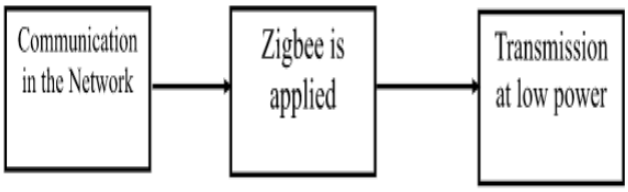
(8) Monitoring based on the neighbor and actual energy using Overhearing technique

Input: Data Dropping attack and False Data injection.
Output: Prevention of attacker node.
Among the SNs if a malicious SN wants to be a CH, so that the node gets higher privilege, the node starts to pretend fake and send fake updates like fake high energy and neighbor count. Once if the malicious SN elects as CH, the performance and integrity of the network gets diminished.



(9) Efficient and Secure Communication Using ZigBee

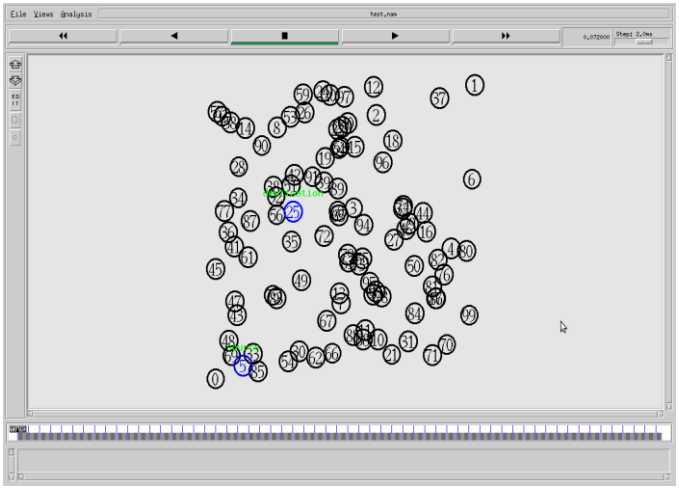
Input: Transmission Ready Packets
Output: Low consumption transmission
In WSNs all the sensors won't work all the time. When the assigned task is done or where there is no work assigned, they are set into sleep mode. Not all the nodes are pushed into sleep mode at a time. Some nodes or the other will keep on monitoring the network based on the available energy. ZigBee based communication is recommended in terms of minimal energy consumption, higher lifetime of network, minimal communication and computational overhead.



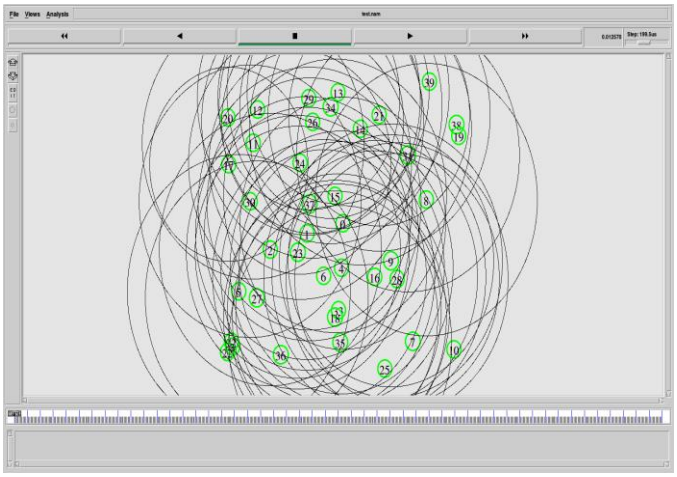
5. Simulation Results

A comparison study is made between the traditional and the proposed technology and the following metrices like Delay, Detection Rate, Communication overhead, Energy consumed, Packet Delivery ratio is extracted using the X graph in NS2 simulator

Wireless Sensor Network



Route Discovery



Source 5: Destination: 25
Node 5 initiates route discovery process to find path for destination 25. It broadcast route request packet to its neighbors. It

attaches the signature in the RREQ packet. Signature is generated using ECC private key. Input for signature is node id. Signature is the encrypted node id. On receiving the RREQ packet, each neighbor accesses the signature and decrypts it is using public key of RREQ sender. If the decrypted signature value matches the sender id, then received RREQ is processed and rebroadcast else the RREQ is dropped.

ECC
Signature Generation and Verification (genuine node)

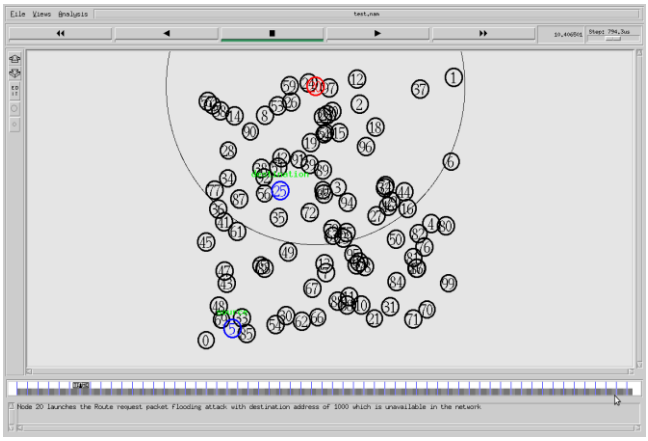
***ECC Signature Generation ***
Genuine node 5 generates signature using its ID
n=185
aa=240 bb=166
Original ID from Source to Receiver: (5)
Node's private key Pb = 166*(189, 81) = (2, 167)
Node's public key Pa = 240*(189, 81) = (112, 44)
Node's private key aa*Pb = 74
Node's public key bb*Pa = 74
Signature from Source to Receiver = {Cyphertext} = {107}

***ECC Signature Verification by node 33 ***
received from 5
Signature input for decryption= 107
Decryption public key bb*Pa = 74
Decrypted Signature from Source = (5)
result=1
Signature is valid. Packet is processed

***ECC Signature Verification by node 69 ***
received from 5
Signature input for decryption= 107
Decryption public key bb*Pa = 74
Decrypted Signature from Source = (5)
result=1
Signature is valid. Packet is processed

Bogus information Injection through Impersonation

Attacker floods the RREQ packet by attaching the destination id as 1000 which is unavailable in the network so that the received RREQ packet will be rebroadcast again and again that floods the network.



ECC
Signature Generation and Verification (attacker node)

***ECC Signature Generation ***
At 6.70 Attacker 20 launches impersonation attack with bogus information injection using genuine node id 12
n=233
aa=63 bb=254
Original ID from Source to Receiver: (12)
Node's private key Pb = 254*(230, 59) = (259, 14)
Node's public key Pa = 63*(230, 59) = (185, 136)
Node's private key aa*Pb = 159
Node's public key bb*Pa = 159
Public key of genuine node bb*Pa = 259
Signature from Source to Receiver = {Cyphertext} = {67}

*** ECC Signature Verification by node 24 ***
received from 12
Signature input for decryption= 67

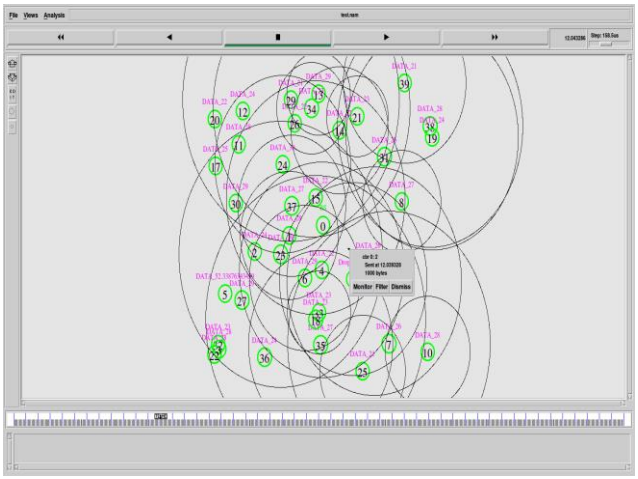
Decryption public key bb*Pa = 259
Decrypted Signature from Source = (49)
result=0
Signature is invalid. Packet is dropped

ECC Signature Verification by node 97
received from 12
Signature input for decryption= 67
Decryption public key bb*Pa = 259
Decrypted Signature from Source = (49)
result=0
Signature is invalid. Packet is dropped

ECC Signature Verification by node 59
received from 12
Signature input for decryption= 67
Decryption public key bb*Pa = 259
Decrypted Signature from Source = (49)
result=0
Signature is invalid. Packet is dropped
Attacker is node 20. It uses the genuine node id 12 and launches impersonation attack to pretend like node 12 performs bogus information injection.

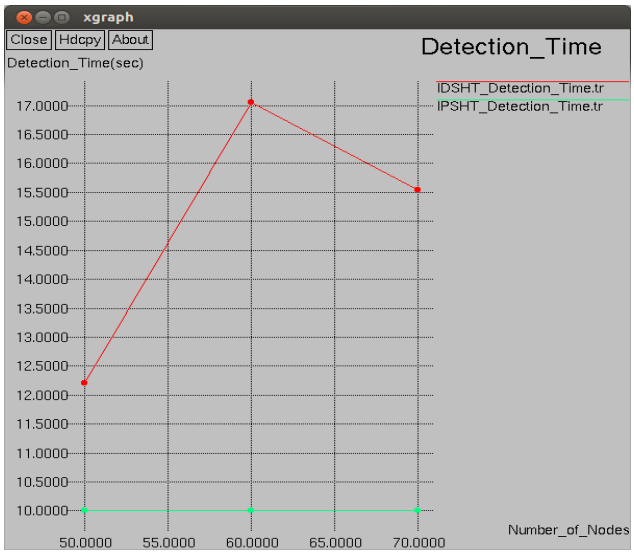
Attacker only uses the ID of node 12 but not private key of 12. Attacker takes node 12 as its input and private key of node 12 for signature generation. Hence all the neighbors that receives the RREQ from node 20 fixes that they received packet from node 12 and utilize the public key of node 12 for signature decryption. Decryption yields mismatched value. Hence the signature is considered as invalid by neighbors, they drop packet and stop rebroadcast. Thereafter flooding is prevented.

False Data Injection Detection



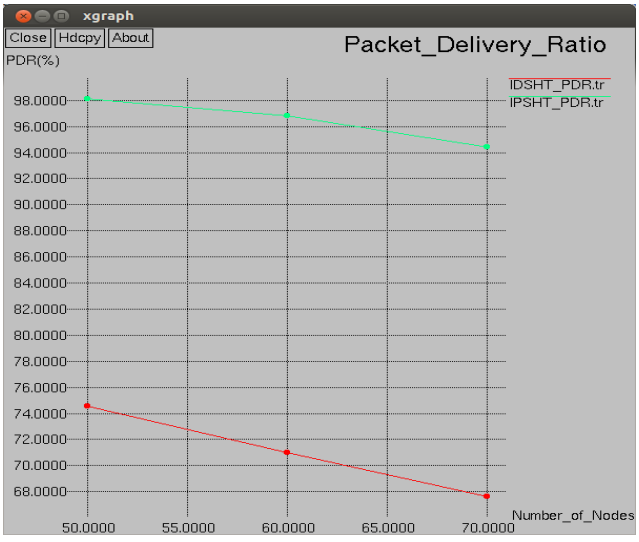
Graph
Detection Time

Due to the prevention mechanism of attacker node in cluster head selection, attacker node is detected at the earlier time during the control information broadcast stage itself. Hence it is completed eliminated during data transmission phase in proposed system. But the attacker cluster head is detected during the data transmission phase in existing system. Hence attack detected time is less in proposed when compared existing system.



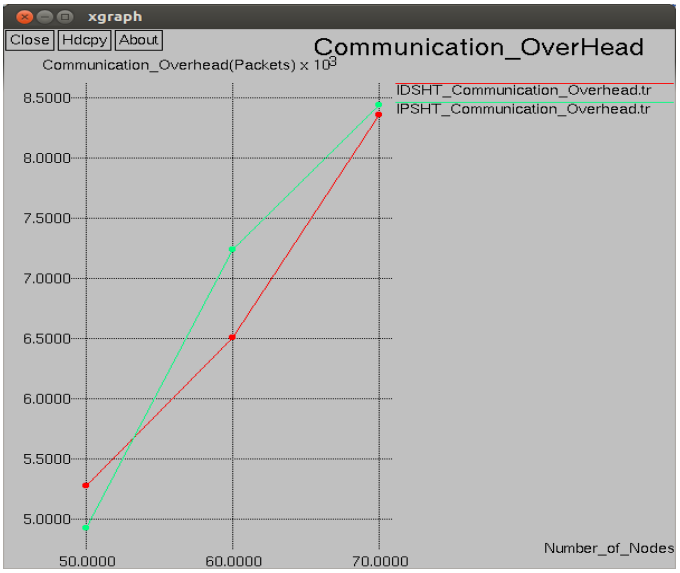
Packet Delivery Ratio

Due to the prevention mechanism of attacker node in cluster head selection, attacker node is detected at the earlier time during the control information broadcast stage itself. Hence it is completed eliminated during data transmission phase in proposed system. Hence packet drop is prevented. But the attacker cluster head is detected during the data transmission phase in existing system. Attacker is detected only after packet dropping. Hence PDR is more in proposed when compared existing system.



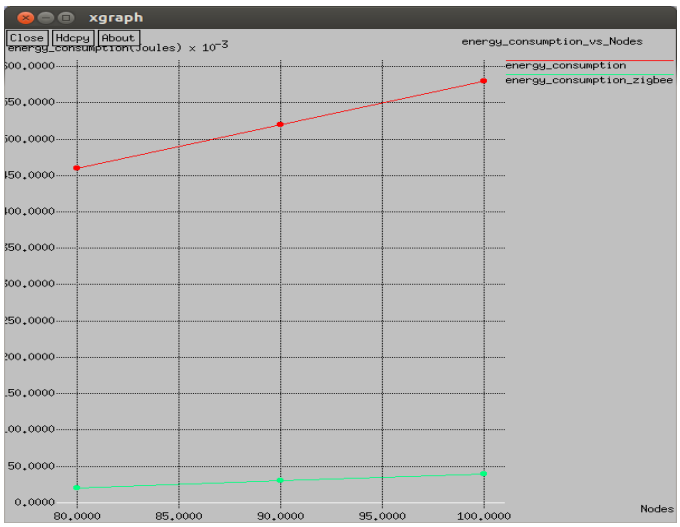
Communication Overhead

In existing system attacker cluster head attracts more neighbors to select it as cluster head with fake control information.

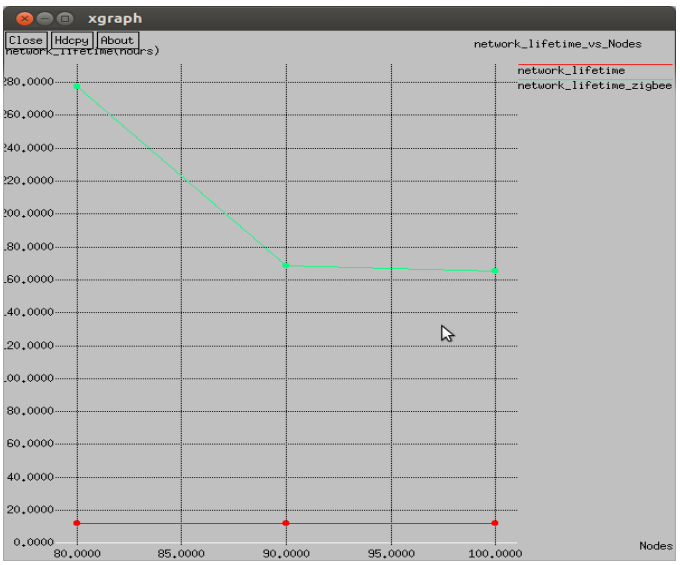


But in proposed system it is prevented. Hence control packet is more in existing when compared to proposed system. In some case both are similar.

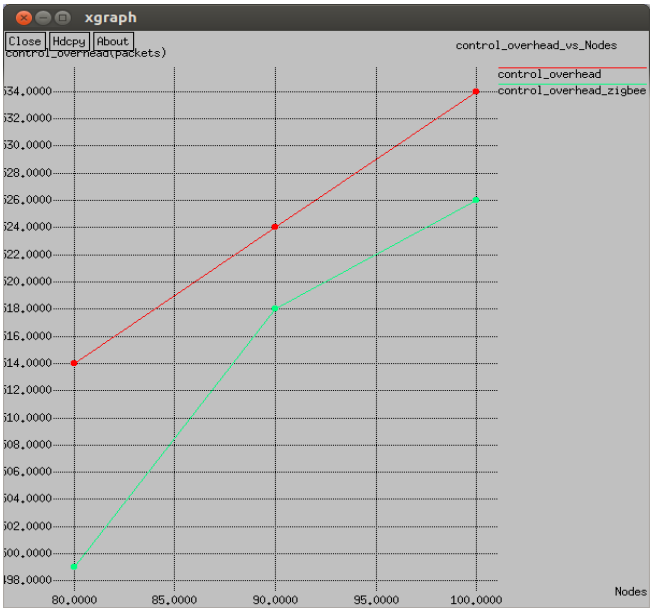
Nodes vs Energy Consumption



Nodes vs Network Lifetime



Nodes vs Control Overhead



6. Conclusion

Proposed Work prevents the bogus information injection attack through signature verification mechanism by using ECC during message broadcast and, false data injection by monitoring the network using overhearing technique. It effectively contributes to detect fake control messages through which the prevention of attack can be done. This is achieved by the statically analyze the energy present and the neighbor count of the nodes among the cluster in WSNs. It also achieves energy efficiency by using the ZigBee Mac standard 802.15.4 at the mac layer that enables low power communication in the resources constrained WSNs. Effectiveness of the proposed approach is evaluated with performance metrices such as overhead, energy consumption, delay ratios through simulation experiments conducted using NS2 simulator. Proposed work provides better performance results and a nugatory scope for future occurring attacks.

References

[1] Zouinkhi, A., Mekki, K. and Abdelkrim, M.N., 2015. Application and network layers design for wireless sensor network to supervise chemical active product warehouse. arXiv preprint arXiv:1501.01193.

[2] Zouinkhi, A., Mekki, K. and Abdelkrim, M.N., 2015. Application and network layers design for wireless sensor network to supervise chemical active product warehouse. arXiv preprint arXiv:1501.01193.

[3] Alrajeh, N.A., Lloret, J. and Canovas, A., 2014. A framework for obesity control using a wireless body sensor network. International Journal of Distributed Sensor Networks, 10(7), p.534760.

[4] Singh, N., Singh, A.K. and Singh, V.K., 2015. Design and performance of wearable ultrawide band textile antenna for medical applications. Microwave and optical technology Letters, 57(7), pp.1553-1557.

[5] Garcia, M., Catalá, A., Lloret, J. and Rodrigues, J.J., 2011, June. A wireless sensor network for soccer team monitoring. In Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011 International Conference on (pp. 1-6). IEEE.

[6] Al-Karaki, J.N. and Kamal, A.E., 2004. Routing techniques in wireless sensor networks: a survey. IEEE wireless communications, 11(6), pp.6-28.

[7] Zhang, Z., Zhu, H., Luo, S., Xin, Y. and Liu, X., 2017. Intrusion Detection Based on State Context and Hierarchical Trust in Wireless Sensor Networks. IEEE Access, 5, pp.12088-12102.

[8] Kohno, E., Ohta, T. and Kakuda, Y., 2009, March. Secure decentralized data transfer against node capture attacks for wireless sensor networks. In Autonomous Decentralized Systems, 2009. ISADS'09. International Symposium on (pp. 1-6). IEEE.

[9] Kohno, E., Ohta, T., Kakuda, Y. and Aida, M., 2011. Improvement of dependability against node capture attacks for wireless sensor networks. IEICE TRANSACTIONS on Information and Systems, 94(1), pp.19-26.

[10] Tanabe, N., Kohno, E. and Kakuda, Y., 2012, November. An impersonation attack detection method using bloom filters and dispersed data transmission for wireless sensor networks. In Green Computing and Communications (GreenCom), 2012 IEEE International Conference on (pp. 767-770). IEEE.

[11] Liu, D. and Ning, P., 2004. Multilevel μTESLA: Broadcast authentication for distributed sensor networks. ACM Transactions on Embedded Computing Systems (TECS), 3(4), pp.800-836.

[12] Liu, D. and Ning, P., 2003, February. Efficient Distribution of Key Chain Commitments for Broadcast Authentication in Distributed Sensor Networks. In NDSS.

[13] Liu, A. and Ning, P., 2008, April. TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks. In Proceedings of the 7th international conference on Information processing in sensor networks (pp. 245-256). IEEE Computer Society.

[14] Duan, M.J. and Xu, J., 2011. An efficient location-based compromise-tolerant key management scheme for sensor networks. Information Processing Letters, 111(11), pp.503-507.

[15] Ren, K., Lou, W., Zeng, K. and Moran, P.J., 2007. On broadcast authentication in wireless sensor networks. IEEE Transactions on Wireless Communications, 6(11).

[16] Gura, N., Patel, A., Wander, A., Eberle, H. and Shantz, S.C., 2004, August. Comparing elliptic curve cryptography and RSA on 8-bit CPUs. In International workshop on cryptographic hardware and embedded systems (pp. 119-132). Springer, Berlin, Heidelberg.

[17] Czypek, P., Heyse, S. and Thomae, E., 2012, September. Efficient implementations of MQPKS on constrained devices. In International Workshop on Cryptographic Hardware and Embedded Systems (pp. 374-389). Springer, Berlin, Heidelberg.

[18] Wang, L. and Xiao, Y., 2006. A survey of energy-efficient scheduling mechanisms in sensor networks. Mobile Networks and Applications, 11(5), pp.723-740.

[19] Yu, M., Malvankar, A. and Foo, S.Y., 2006, June. An energy-efficient path availability routing algorithm for mobile ad hoc sensor networks. In Communications, 2006. ICC'06. IEEE International Conference on (Vol. 4, pp. 1885-1890). IEEE.

[20] Jardosh, S. and Ranjan, P., 2008, January. A survey: Topology control for wireless sensor networks. In Signal Processing, Communications and Networking, 2008. ICSCN'08. International Conference on (pp. 422-427). IEEE.

[21] Varga, A. and Hornig, R., 2008, March. An overview of the OMNeT++ simulation environment. In Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops (p. 60). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[22] Howitt, I. and Gutierrez, J.A., 2003, March. IEEE 802.15. 4 low rate-wireless personal area network coexistence issues. In Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE (Vol. 3, pp. 1481-1486). IEEE.

[23] Xia, C., Liu, W. and Deng, Q., 2015. Cost minimization of wireless sensor networks with unlimited-lifetime energy for monitoring oil pipelines. IEEE/CAA Journal of AutomaticaSinica, 2(3), pp.290-295.

[24] Qinqin, Z.Y.L.Z.W., 2005. ZigBee Wireless Communication Technology and Investigation on Its Application [J]. Process Automation Instrumentation, 6, p.002.

[25] Aalto, L., Göthlin, N., Korhonen, J. and Ojala, T., 2004, June. Bluetooth and WAP push based location-aware mobile advertising system. In Proceedings of the 2nd international conference on Mobile systems, applications, and services (pp. 49-58). ACM.

[26] Khedo, K.K., Perseedoss, R. and Mungur, A., 2010. A wireless sensor network air pollution monitoring system. arXiv preprint arXiv:1005.1737.

[27] Butun, I., Morgera, S.D. and Sankar, R., 2014. A survey of intrusion detection systems in wireless sensor networks. IEEE communications surveys & tutorials, 16(1), pp.266-282.
[28] Ghaffari, A., 2015. Congestion control mechanisms in wireless sensor networks: A survey. Journal of network and computer applications, 52, pp.101-115.
[29] Shen, H., He, S., Yu, L. and Sarker, A., 2017, March. Prediction-based redundant data elimination with content overhearing in wireless networks. In Pervasive Computing and Communications (PerCom), 2017 IEEE International Conference on (pp. 50-58). IEEE.
[30] Sett, R. and Banerjee, I., 2015, August. An overhearing based routing scheme for Wireless Sensor Networks. In Advances in Computing, Communications and Informatics (ICACCI), 2015 International Conference on (pp. 2076-2082). IEEE.
[31] Abbasi, A.A. and Younis, M., 2007. A survey on clustering algorithms for wireless sensor networks. Computer communications, 30(14-15), pp.2826-2841.
[32] Shim, K.A., 2017. BASIS: A practical multi-user broadcast authentication scheme in wireless sensor networks. IEEE Transactions on Information Forensics and Security, 12(7), pp.1545-1554.
[33] Tanabe, N., Kohno, E. and Kakuda, Y., 2013, July. A path authenticating method using bloom filters against impersonation attacks on relaying nodes for wireless sensor networks. In Distributed Computing Systems Workshops (ICDCSW), 2013 IEEE 33rd International Conference on (pp. 357-361). IEEE.
[34] Chang, Q., Zhang, Y.P. and Qin, L.L., 2010, June. A node authentication protocol based on ECC in WSN. In Computer Design and Applications (ICCDA), 2010 International Conference on (Vol. 2, pp. V2-606). IEEE.
[35] Mahmood, Z., Ning, H. and Ghafoor, A., 2016, December. Lightweight Two-Level Session Key Management for End User Authentication in Internet of Things. In Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016 IEEE International Conference on (pp. 323-327). IEEE.
[36] Ding, C., Yang, L. and Wu, M., 2015, December. LFDD: Local False Data Detection for In-Network Aggregation in Wireless Sensor Networks. In Computational Intelligence and Design (ISCID), 2015 8th International Symposium on (Vol. 2, pp. 262-266). IEEE.
[37] Sett, R. and Banerjee, I., 2015, August. An overhearing based routing scheme for Wireless Sensor Networks. In Advances in Computing, Communications and Informatics (ICACCI), 2015 International Conference on (pp. 2076-2082). IEEE.
[38] Ye, W., Heidemann, J. and Estrin, D., 2002. An energy-efficient MAC protocol for wireless sensor networks. In INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE (Vol. 3, pp. 1567-1576). IEEE.
[39] Kurtoglu, A., Carletta, J. and Lee, K.S., Energy Consumption in Long-Range Linear Wireless Sensor Networks using LoRaWan and ZigBee.
[40] Siraj, S., Gupta, A. and Badgujar, R., 2012. Network simulation tools survey. International Journal of Advanced Research in Computer and Communication Engineering, 1(4), pp.199-206.
[41] Misra, S., Das, S. and Obaidat, M., 2014. Context-aware quality of service in wireless sensor networks. IEEE Communications Magazine, 52(6), pp.16-23.
[42] Younis, O. and Fahmy, S., 2004. HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. IEEE Transactions on mobile computing, 3(4), pp.366-379.
[43] Araghi, T.K., Zamani, M. and Mnaf, A.B.A., 2013, September. Performance analysis in reactive routing protocols in wireless mobile ad hoc networks using DSR, AODV and AOMDV. In Informatics and Creative Multimedia (ICICM), 2013 International Conference on (pp. 81-84). IEEE.
[44] Mo, Y., Garone, E., Casavola, A. and Sinopoli, B., 2010, December. False data injection attacks against state estimation in wireless sensor networks. In Decision and Control (CDC), 2010 49th IEEE Conference on (pp. 5967-5972). IEEE.
[45] T. Padmapriya and V.Saminadan, “Improving Performance of Downlink LTE-Advanced Networks Using Advanced Networks Using Advanced feedback Mechanisms and SINR Model”, International Conference on Emerging Technology (ICET), vol.7, no.1, pp: 93, March 2014.
[46] S.V.Manikanthan and K.srividhya "An Android based secure access control using ARM and cloud computing", Published in: Electronics and Communication Systems (ICECS), 2015 2nd International Conference on 26-27 Feb. 2015,Publisher: IEEE,DOI: 10.1109/ECS.2015.7124833.