Developing an Improvised Secured Routing Protocol for WSNSUsing Hierarchical & Clustered Approach

Pranav Pradip Chippalkatti[1]
Research Scholar VTU RRC Belagavi

Swagat Madhav Karve[2]
Research Scholar VTU RRC Belagavi

Rajesh Maharudra Patil[3]
Co-Supervisor, VTU RRC Belagavi

Dr. Nagaraja[4]
B.G. Jain Institute of Technology,
Devanagere

Article Info
Page Number: 1884 - 1900
Publication Issue:
Vol 70 No. 2 (2021)

Abstract

This paper is related to the developing of an improvised secured routing protocol for WSNs using hierarchical & clustered approach. NS2 is used as the simulation tool to simulate the outputs. The simulation results shows the effectivity of the methodology that is being proposed by us.

Article History
Article Received*: 05 September 2021*
Revised*: 09 October 2021*
Accepted*: 22 November 2021*
Publication*: 26 December 2021*

Keywords **–** WSN, Static, Dynamic, Packets, Authentication, Sensor, Node, Distribution, Network, Key, Message Authentication Code Protocol, Security, Routing, Management, Sink, Cryptography, Source, Energy, Router, Attacker, Base Station, Machine condition monitoring, Industrial wireless sensor networks.

I. Introduction

Wireless sensor networks (WSNs) consist of many sensor nodes capable of wireless communication and data collection. In addition to sensor nodes, most WSNs include two other components, which are base station and cluster head. Key encryption technology is a basic technique for protecting the secrecy of transmitted data among sensor nodes in wireless sensor networks. Sensor nodes are limited by insufficient hardware resources, such as memory capacity, battery lifetime, and processor speed [4].

The limitations of memory determine the amount of data to be stored, while battery lifetime determines the life of sensor nodes and slow processors cannot handle complex computations. These problems in turn will influence the efficiency of sensor networks. As a result, few current key management schemes are appropriate for wireless sensor networks [3]

Regarding the security issues in the wireless sensor network, the encrypting scheme must not increase the load of sensor nodes. If sensor nodes need to perform complex computations for encryption, it would consume the energy of sensor nodes. Hence, the traditional encrypting and decrypting method is not suitable for wireless sensor networks [1].

II Proposed methodology - Solve security issue

In his paper, a new key management method that uses dynamic key management schemes for heterogeneous sensor networks is being proposed. The members of this network include a minority of powerful high-end sensors (H-sensors), which work as cluster heads, and a majority of low-end sensors (L-sensors). The high-end sensors have more memory, a wider transmission range, longer battery and greater fault tolerance. Low-end sensors represent general sensor nodes [5].

In the proposed method, the L-sensors only store a little data at a time. Hence, they only require a little memory to work quickly. H-sensors regularly replace the encrypting key based on the status of the cluster. At the same time, the L-sensors can determine if the new key is legal. This design requires fewer resources to achieve the security of sensor nodes in wireless sensor networks, while ensuring confidentiality, integrity, and availability [6]. The proposed scheme loads a hash function into the base station, cluster heads, and sensor nodes. The cluster heads and sensor nodes then generate their own key chains to provide forward authentication in case of key changes, security breaches, and key changes due to security breaches. The cluster heads and sensor nodes establish pair-wise keys to ensure transmission secrecy. The proposed scheme decreases the number of keys required for sensor nodes and cluster heads and is robust to the following attacks: guessing attacks, replay attacks, man-in- the-middle attacks, node capture attacks, and denial-of- service attacks [2].

III Background literature

Some of the authors have worked in the topic chosen in this paper, which are put forth here one after the other in succession. The authors L. Kejie, Q. Yi, and H. Jiankun worked a lot on the frameworks for distributed key management scheme/s in *w*-HSNW's & devised various protocols to tackle the security issues. Here, they also worked on the key management schemes in distributed wireless sensor networks with heterogeneous sensor nodes. In homogeneous sensor networks, all sensor nodes have the same characteristics, such as battery lifetime, computation power, and memory capacity. However, some proposed key management schemes for homogeneous sensor networks encounter the problems of low transmission speed, limited scalability, and a lack of fault tolerance. Heterogeneous sensor networks (HSNs) can avoid these problems. In HSNs, which include several kinds of sensor nodes, different kinds of sensor nodes have different properties and transmission ranges. Their work suffered from major drawbacks such as [7]

- Memory capacity to be maximized
- Battery lifetime to be increased
- Scalability to be increased (Need to analyze with huge number of heterogeneous nodes)

The research team led by X. Du, Y. Xiao, M. Guizani and H.H. Chen proposed an effective key management scheme for HSNs and showed that the key management is an essential cryptographic primitive to provide security operations. Here, they presented an effective key management scheme that takes advantage of the powerful high-end sensors in heterogeneous sensor networks. The performance evaluation and security analysis show that the key management scheme provides better security with low complexity and significant reduction on storage requirement, compared with existing key management schemes, but their work suffered from certain disadvantages such as [8]

- Communication and computation overhead

- High energy requirement
- Performance to be increased

Research engineers team led by D. Liu and P. Ning worked on the loocation-based pair-wise key establishments for static WSN's where, they presented a simple location-aware deployment model & developed two pair-wise key pre-distribution schemes by taking advantage of sensors' expected locations, aiming atimproving pair-wise key establishment in sensor networks. When sensors in a network can be deployed to the expected locations with a certain precision, these schemes provide better security and performance over the previous solutions. The First scheme, closest pair-wise keys scheme, is resistant to node capture attacks and has no limit on the total number of sensors. Its extended version further reduces the storage overhead and simplifies the dynamic deployment of new sensors. The second scheme, location- based key pre-distribution using polynomials, employs a threshold technique and provides a trade-off between the security against node capture and the performance of establishing pair-wise keys. Their work suffered from a number of lacunas & some of them were [9]

- Security to be increased
- Deployment error to be decreased
- Performance to be increased

Famous South Asian networking engineers, Y. Zhang,
W. Liu, W. Lou and Y. Fang researched upon the topic of securing sensor networks with location-based keys in heterogeneous nets & the trio propose the novel notion of location-based keys for designing compromise-tolerant security mechanisms for sensor networks. Based on location based keys, they develop a node-to-node authentication scheme, which is not only able to localize the impact of compromised nodes within their vicinity, b also to facilitate the establishment of pair-wise keys between neighboring nodes. This scheme has perfect resilience against node compromise, low storage overhead, and good network scalability. Also demonstrate the use of location-based keys in combating a few notorious attacks against sensor network routing protocols. Certain drawbacks were found in their works, which were [10]

- Need evaluate the performance of this scheme inpractical sensor networks.
- Need to investigate the potential applications oflocation-based keys in securing sensor networks.

A. Wadaa, S. Olariu, L. Wilson and M. Eltoweissy devised cryptographic key management system in h- WSNs using scalable concepts. The authors proposed a scalable key management scheme for sensor networks consisting of a large-scale random deployment of commodity sensor nodes that are anonymous. The proposed scheme relies on a location-based virtual network infrastructure and is built upon a combinatorial formulation of the group key management problem. Primary features of this scheme include autonomously computing group keys, and dynamically computing, using a simple hash function, the mapping of nodes to group keys. The scheme scales well in the size of the network and supports dynamic setup and management of arbitrary structures of secure group communications in large-scale wireless sensor network. Some drawbacks in their works were [11]

- Performance to be increased
- Need to decrease the energy requirement

- Security to be increased

D. Liu, P. Ning and W. Du worked on many of the key pre-distribution techniques that take the advantage of sensors' expected locations to help pre-distributing keying materials in huge *h*-WSNs. However, it is usually very difficult, and sometimes impossible, to guarantee the knowledge of sensors' expected locations. In order to remove the dependency on expected locations. They worked on the group-based key pre-distribution & proposed a practical deployment model, where sensor nodes are deployed in groups, and the nodes in the same group are close to each other after the deployment. Based on this model, the paper develops a novel group-based key pre-distribution framework, which can be combined with any of existing key pre-distribution techniques. A distinguishing property of this framework is that it does not require the knowledge of sensors' expected locations and greatly simplifies the deployment of sensor networks. Even though there were good advantages, equal number of disadvantages were there in their proposed work [12]

- Memory capacity to be maximized
- Performance to be increased
- Complexity to be decreased

Networking team research led by M.F. Younis, K. Ghumman and M. Eltoweissy worked on the location-aware combinatorial key management scheme for clustered WSNs & focussed on the management of encryption keys in large-scale clustered *h*-WSNs. The authors proposed a novel distributed key management scheme based on exclusion basis systems (EBS) along with a combinatorial formulation of the group key management problem. This scheme is termed SHELL because it is scalable, hierarchical, efficient, location-aware, and light- weight. Unlike most existing key management schemes for WSNs, SHELL supports rekeying and, thus, enhances network security and survivability against node capture. SHELL distributes key management functionality among multiple nodes and minimizes the memory and energy consumption through trading off the number of keys and rekeying messages. In addition, SHELL employs a novel key assignment scheme that reduces the potential of collusion among compromised sensor nodes by factoring the geographic location of nodes in key assignment. The deficits found in their work were [13]

- Memory requirement to be minimized
- Performance to be increased

IV Main objectives of the proposed work

The main objective of the proposed work is to develop a high secured forward authentication key management concept for a heterogeneous WSN. Wireless sensor networks (WSNs) consist of many sensor nodes capable of wireless communication and data collection. In addition to sensor nodes, most WSNs include two other components, which are base station and cluster head. Key encryption technology is a basic technique for protecting the secrecy of transmitted data among sensor nodes in wireless sensor networks. However, sensor nodes are inherently limited by insufficient hardware resources such as memory capacity and battery lifetime. As a result, few current key management schemes are appropriate for wireless sensor networks. This paper proposes a new key management method that uses dynamic key management schemes for heterogeneous sensor networks. The proposed scheme loads a hash function into the base station, cluster heads, and sensor nodes. The cluster heads and sensor nodes then generate their own key chains to provide forward authentication in case of key changes, security breaches,

and key changes due to security breaches. The cluster heads and sensor nodes establish pair-wise keys to ensure transmission secrecy. The proposed scheme decreases the number of keys required for sensor nodes and cluster heads and is robust to the following attacks: guessing attacks, replay attacks, man-in-the-middle attacks, node capture attacks and denial-of-service attacks [14].

V Concepts used in security process

The proposed method includes [15]

- key revocation,
- addition of a new node, and
- the generation of a new key-chain. which are given a small insight to it as below.

Key Revocation : In HSNs, if the BS discovers a compromised node or adversary (assume that the BS has an intrusion detection system mechanism inside), the BS broadcasts the "Malicious node message" to all the H-sensors.

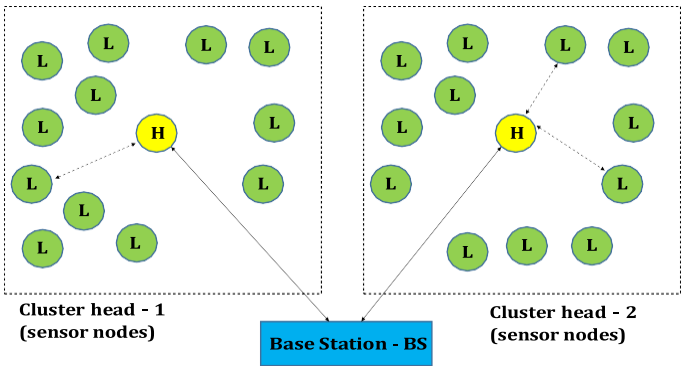

Fig. 1 : The architectural layout of the heterogeneous sensor network used in our research work

Addition of a New Node : The newly deployed node needs to establish pair-wise key with its own H-sensor. Before adding new node into an environment, this new node should be ensured that it is not a comprised node and the hash function and the temporary session key are securely stored. After the deployment of a new L-sensor node, the BS actively delivers the "new node message" about the addition of a new node to all H-sensors.

Generation of a New Key-Chain : When the last key in the key-chain has been used in the cluster, as long as H- sensor still has sufficient power, it creates a new key-chain for the L-sensors in the cluster. H-sensor uses the pair-wise key to encrypt the new key for the L-sensors.

VI Technical details of the proposed work

Here, in this section, a key-chain protocol for key management is developed for HSN's. Each cluster head generates its own key-chain, which encrypts messages and communicates with the other sensor nodes in the cluster. Based on hierarchical clustering, each cluster consists of several sensor nodes and a cluster head. Several clusters and a base station form the heterogeneous sensor networks which is shown in the Fig. 1 & 2 respectively 1 along with the technical details in Fig. 3 [16].

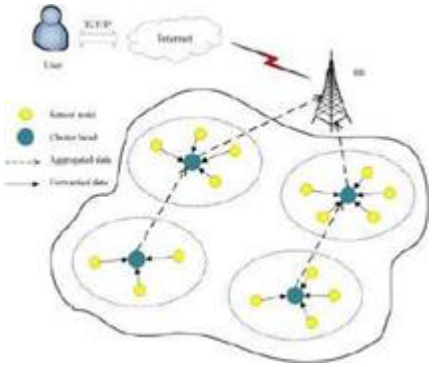

Fig. 2 : Forward authentication key management scheme for *h*-WSNs

There are 2 types of sensors in hierarchical clustering HSNs, viz.,

1. a small number of powerful high-end sensors (H-sensors, the same as the cluster head) and
2. a large number of low-end sensors (L-sensors, the same as the ordinary sensor node).

The H-sensors are equipped with tamper resistant hardware and have more memory and greater processing capability. They can communicate directly with the base station. The L-sensors are normal sensor nodes that are limited in terms of processing capability, power, and memory. L-sensors acquire data from the surrounding environment and forward the collected data to the H-sensors. The H-sensors can communicate directly with the base station; all the L-sensor packets are transmitted to the BS via the H-sensor. This approach assumes that the base station is trusted.

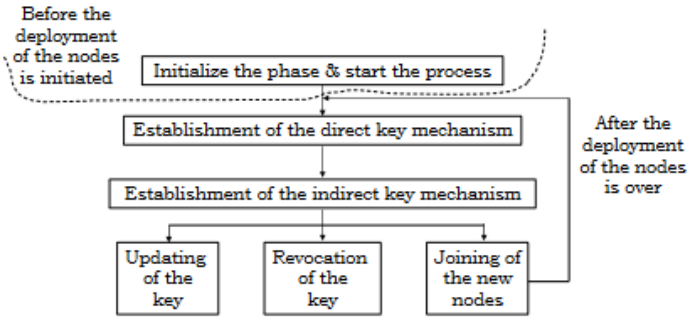

Fig. 3 : The main layout of the developed key management scheme

The proposed system assumes the following 5 important communication protocoled rules. These communication rules should be followed in order to avoid a compromised node infringing the other L-sensors and to prevent the attacks such as

replay attacks or man-in-the middle attacks. Those 5 important communication protocols are [17]

1. H-sensors can directly communicate with the BS.
2. The base station exchanges messages with L-sensors through H-sensors and vice versa.
3. H-sensors can send messages to specific L-sensors in the cluster.
4. H-sensors can broadcast messages to all L-sensors in the cluster.
5. L-sensors must exchange the messages with each other through an H-sensor. In other words, L-sensors cannot directly exchange messages with each other. Hence, a compromised L-sensor cannot affect the other L-sensor in the cluster.

VII Initialization & authentication phases

In the work considered, the keying protocol developed w.r.t. the HSNs are carried out in two phases, initialization and authentication phase, which are explained as under 1. Initialization Phase: The base station generates a key pool before deployment of L-sensors and H-sensors. The base station then chooses a unique key for each H-sensor, which is regarded as cluster key HK.

Authentication Phase: After all nodes are distributed in the environment, the H-sensors decide which nodes to connect with.

VIII Input datasets & expected results

Input : Message

Output : We analyse the proposed method from the following 3 issues : management scheme

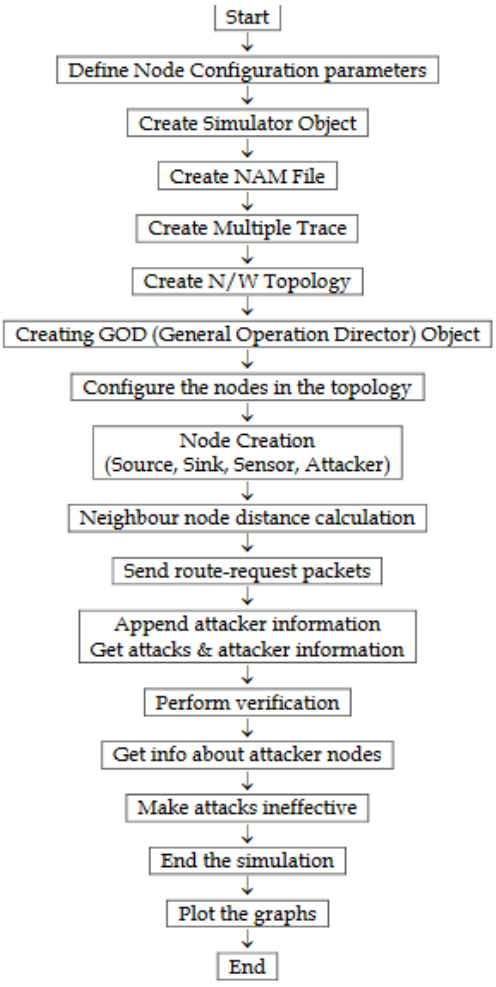

Fig. 4 : Flow chart / Data flow diagram used in ourcoding process

1. the number of messages for grouping andestablishing the pair-wise key;
2. the key sizes;
3. the power consumption analysis.

1. **The Number of Messages between the H-Sensor and L-Sensor:** In the proposed scheme, each H-sensor establishes a pair-wise key with its own L-sensor and three messages are exchanged: the H-sensor broadcasts two messages, and an L-sensor node sends one response message. In

updating the key, the H- sensor and L-sensor nodes only send one message, where the H-sensor node broadcasts the hello message.

2. **The Key Sizes:** In the proposed scheme, regardless of the number of L-sensor nodes, each L-sensor only stores three keys. This approach reduces memory space requirements and increases the efficiency of each sensor node.

3. **Power Consumption Analysis:** For each sensor node, the costs of the energy consumption are primarily in data transmission and receiving. In our scheme, we assume that a packet consists of 16-byte MAC (the size of hash, 128 bit), 16-byte payload, 20-byte header, and 10-byte preamble. The total length of packet is 62 bytes. Each L-sensor node is assigned an initial energy of 1 J, and the power consumption for receiving and transmitting one byte of packet is assumed to be 28.6 □J and 59.2 □J respectively [18].

IX NS-2 Simulation Results

In this research work, we have proposed an improvised secured routing protocol for WSNs using hierarchical & clustered approach. The coding (script writing) for the development of a cooperative wireless sensor networks for efficient data transfer schemes is developed in the **.**NS2 tool by writing **.**tcl scripts and once it is completed, it is tested for its effectiveness as per the algo steps given below as per the flow chart shown in the Fig. No. 4. Next, the developed code is saved in a particular folder in the Ubuntu environment as shown in the Fig. 5. The Ubuntu is started next.

At the terminal, commands like sudo –s is being used to enter the kernel (Fig. 8) The password is being set. Next, the source code in which the directory / folder is present is changed using cd command. The developed code is run using ns filename**.**tcl. The command window of the NS-2 simulator appears with the simulator start button along with the network animator as shown in the Fig. 9. Once the simulation is started, the node deployment within the 'n' number of cluster heads along with the base station, sink, etc…. on the NS-2 animator screen as shown in the Figs. 10 & 11 respectively along with the attacker nodes [19].

The proposed algorithm developed is incorporated in the .tcl file in the NS2 environment. The coding is developed in such a way that 40 sensor nodes are deployed in the network similar animator window, the code pattern can be observed in the Fig. 6 & 7 respectively. The data transfer starts from the source node by sending "*hello*" packets to the sink via the nodes as shown in the Figs. 12 & 13 respectively.

Once the data transfer starts, attacker nodes starts attacking in the middle & starts to steal the information, but the proposed algorithm immediately identifies which nodes has been attacked by the attacker, ensures the keying is done in a proper manner and immediately makes the effect of attacking node on the attacked node ineffective and the normal process of the data packet transfer starts.

Simulation takes couple of minutes, passes different stages of data packets sending, verification, encryption, decryption from the source node S-D to the sink or destination node. Once the data transfer is fully successful, the final step is to observe the simulated results from the NAM window command prompt by using the commands chmod 777 results.sh & running the shell script ./results.sh & the plots of throughput, packet delivery, packets drop, etc… are plotted & the results are analyzed from which we can come to a conclusion that there is zero packets drop, say if 10 packets are sent from the source, at the receiving end also, it is 10, thus the drop is 10 – 10 = Zero [20].

Fig. 5 : Folder showing all the relevant files developed forin the Ubuntu environment

Fig. 6 : Structure of the main program “main.tcl” showingthe syntaxes, blue shows the steps involved in the development of the code

Fig. 7 : Part of the “main.tcl” code showing the intermediate steps such as configuration & creation of thesensor & attacker nodes

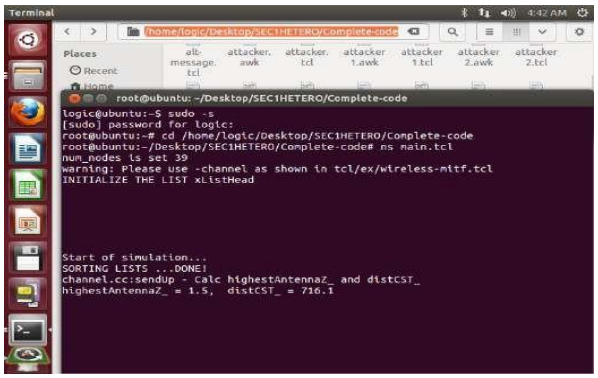

Fig. 8 : Running the main file @ the terminal point byexecuting the command ; ns main.tcl @ the commandprompt

Fig. 9 : Activation of the NAM window & the NAMsimulator window once the main file is evoked

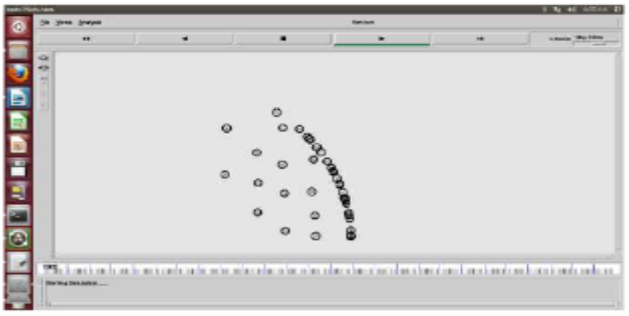

Fig. 10 : Deployment of the nodes showing the start of thesimulation

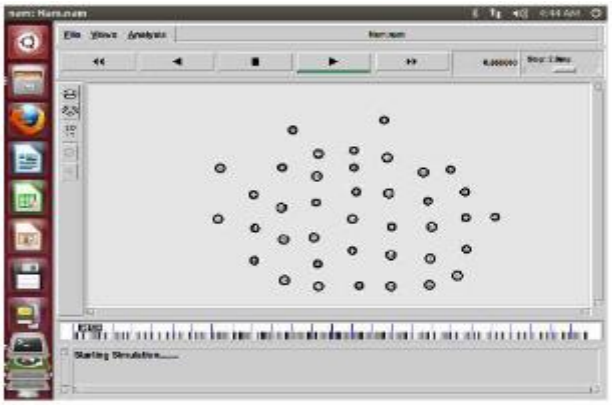

Fig. 11 : Complete deployment of all the nodes along withsensor nodes, sink node, source node, attacker nodes

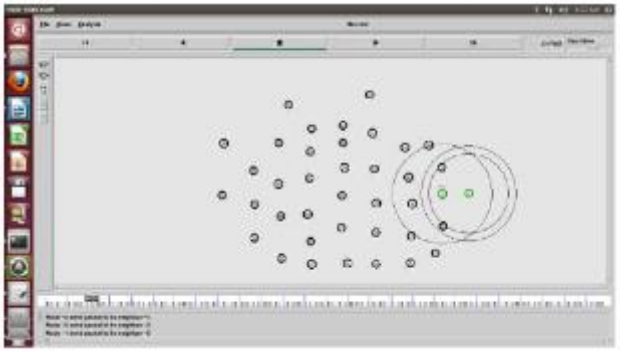

Fig 12 : Source node starting the despatch of the ‘hello’ message packets to the sink via the neighbouring nodes (shown in concentric circles), say node 0-sending packetsto neighbour 1, to 3, etc….

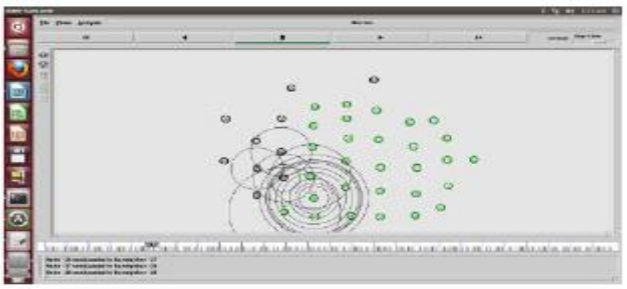

Fig 13 : Source node starting the despatch of the 'hello' message packets to the sink via the neighbouring nodes (shown in concentric circles), say node 26-sending packets to neighbour 27, node 27 to node 26, node 28 to node node26 … . & so on.

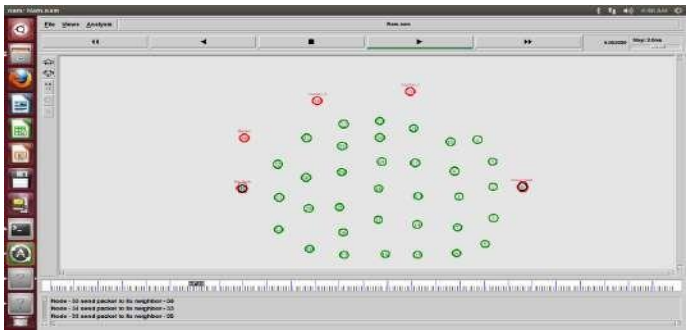

Fig. 14 : Simulation showing the 2 attacker nodes (37 &38) coming suddenly into the picture during the data transmission

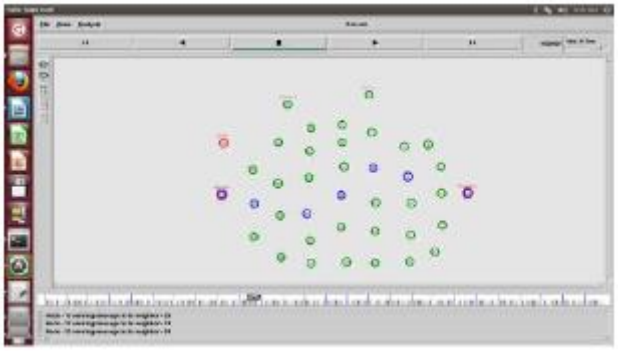

Fig. 15 : Data transfer from s to d taking place successfullyin spite of attacker nodes (showing no effect)

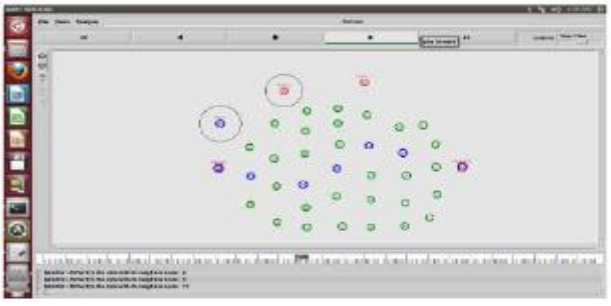

Fig. 16 : Attacker-1 (node 28) springing into action,whereas node 36 monitoring the situation & authenticating the keys to the nodes to be careful

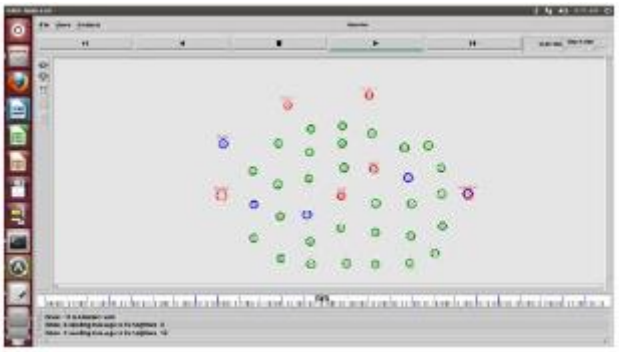

Fig. 17 : Attacker nodes attacking the nodes 12 & 18(before attacking)

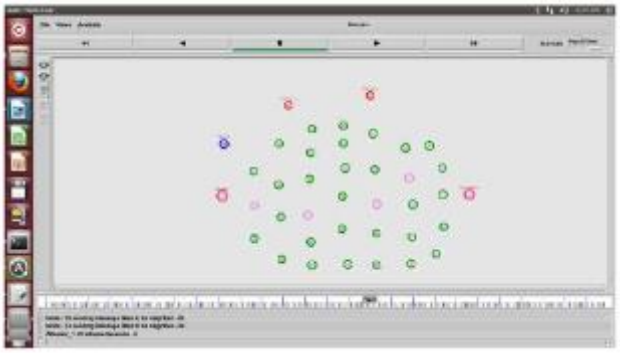

Fig. 18 : Attacker nodes attacking the nodes 12 & 18 (afterattacking, the sensor nodes 12 & 18 become active again due to the algorithm developed showing the ineffectiveness of the attacker nodes on the sensor nodes
…. showing the security is good)

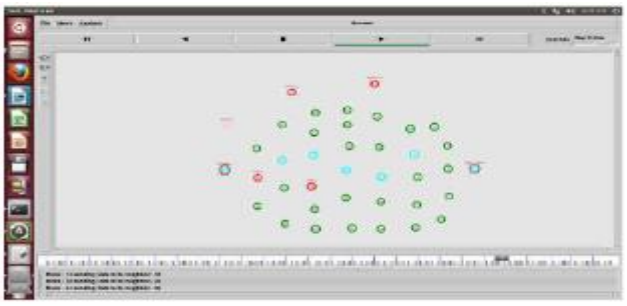

Fig. 19 : Source sending the data to the sink via a newrouting path, 2 attacker nodes attacking node 33 & 25(showing red)

Fig. 20 : Source sending the data to the sink via a new routing path, 2 attacker nodes attacking node 33 & 25 (showing red), again attacking another 2 nodes 30 & 24(showing green)

Fig. 21 : Data transfer from s to d via the new path successfully inspite of attaching the nodes in the path (proposed algorithm takes care of the attacked nodes which have been attacked by the attackers & making itinactive, thus showing the security levels)

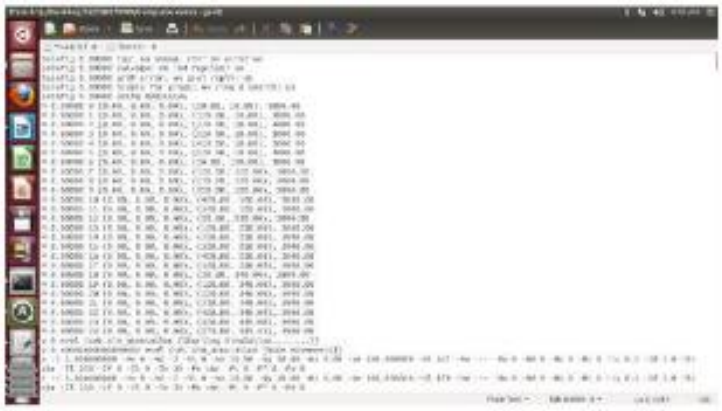

Fig. 22 : Trace file showing all the datas, how much data packets has been transferred, how much time taken to move from s to d inspite of attackers attacking the nodesin the path

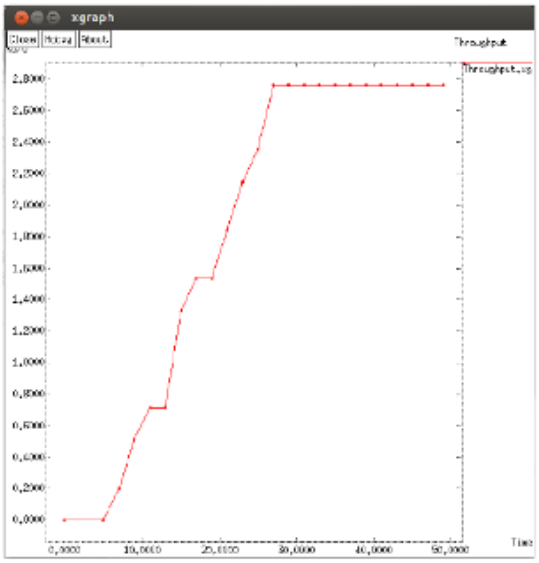

Fig 23 : Plot of throughput obtained v/s time

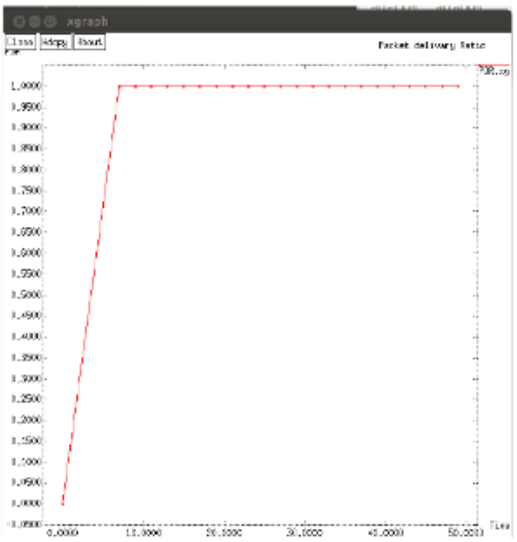

Fig. 24 : Plot of packet delivery ratio or the verification failure rate obtained v/s time

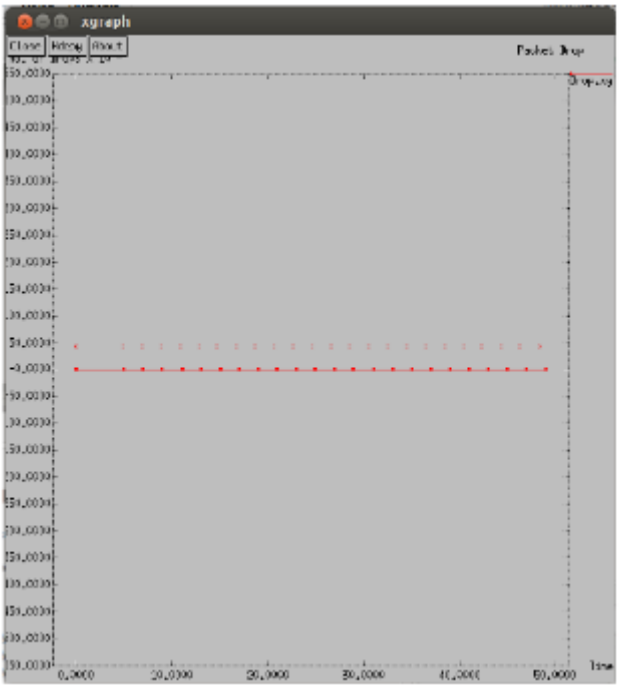

Fig. 25 : Plot of fraction of packets dropped obtained v/s time

X Conclusion

In the research work presented in this paper, routing protocol development for a heterogeneous wireless sensor network using the concepts of key encryption, key revocation, addition of a new node & and the generation of a new key-chain w.r.t. base station and cluster heads is being presented. Finally, the main aim of this work was to present a new key management scheme that is suitable for HSNs inspite of attacker nodes. This study proposes a new key management scheme that is suitable for HSNs. By clustering all the sensor nodes in the environment, cluster heads can generate their own key-chain, which can be seen in the simulated results. The key chain helps in the data transfer of the packets.

The sensor nodes and their cluster heads can jointly establish pair wise keys. Pair wise keys ensure

transmission secrecy for each message, protecting data integrity and determining if the sensor nodes are malicious. The key-chain consists of continuous keys, and each key is dependent. This makes it possible for the sensor node to confirm the validity of each key. Sensor nodes or cluster heads through the characteristic of key-chain, when the cluster heads change the key, and then sensor nodes can confirm the identity of the cluster head and the validity of new key. In our scheme, the key is calculated by hash function. The hash function makes it possible to compress data into a fixed length and avoid data collision. Sensor nodes only need to store a few keys and a hash function at a time, reducing the memory requirements of sensor nodes and ensuring key security. The simulation results shows the effectiveness of the methodology that is being developed in this paper.

References

[1] Muhammad Nadeem Akhtar, Arshad Ali, Zulfiqar Ali, Muhammad Adnan Hashmi, Muhammad Atif, "Cluster Based Routing Protocols for Wireless Sensor Networks: An Overview*", International Journal of Advanced Computer Science and Applications* (IJACSA), Vol. 9, No. 12, 2018.

[2] Singh S.K., Singh M.P. & Singh, Dharmendra, "A survey of energy-efficient hierarchical cluster-based routing in wireless sensor networks", *International Journal of Advanced Networking and Application* (*IJANA*), Vol. 2, pp. 570-580, 2010.

[3] Bilal Jan, Haleem Farman, Huma Javed, Bartolomeo Montrucchio, Murad Khan and Shaukat, "Energy Efficient Hierarchical Clustering Approaches in Wireless Sensor Networks: A Survey", *Hindawi Wireless Communications and Mobile Computing*, Vol. 2017, Article ID 6457942, 14 pages, 2017.

[4] Method Gajendran Malshetty, Basavaraj Mathapati, "WSN Clustering Based on EECI (Energy Efficient Clustering using Interconnection)", *International Journal of Innovative Technology and Exploring Engineering* (*IJITEE*), *Published By: Blue Eyes Intelligence Engineering & Sciences Publication*, ISSN: 2278-3075, Vol. 9 Issue 1, pp. 3564, Madhya Pradesh, India, Nov. 2019.

[5] Pavithra G.S., Babu N.V., "Energy Efficient Hierarchical Clustering using HACOPSO in Wireless Sensor Networks", *International Journal of Innovative Technology and Exploring Engineering* (*IJITEE*) ISSN: 2278-3075, Vol. 8 Issue 12, pp. 5219-5225, October, 2019.

[6] Thesiya Khushbu , Viraj Daxini, "Novel Clustering Approach to Reduce Energy Consumption in Wireless Sensor Network based on LEACH", *International Journal of Computer Science and Mobile Computing*, Vol. 4 Issue 6, pg. 945-953, Jun. 2015.

[7] A. Babu Karuppiah, J. Dalfiah, "An Improvised Hierarchical Black Hole Detection Algorithm In Wireless Sensor Networks", *IOSR Journal of Electronics and Communication Engineering* (*IOSR-JECE*) e-ISSN: 2278- 2834,p- ISSN: 2278-8735, (ICEICT 2016), Second International Conference on Electrical, Information and Communication Technology, pp. 134-141, 2016.

[8] Ganesh, "Efficient and secure routing protocol for wireless sensor network", *Ph.D. Thesis*, *Sathyabama University*, Jeppiaar Nagar, Chennai-119, India, August 2014.

[9] Rajesh Kumar Varun, R.C. Gangwar, "Hierarchical Energy Efficient Routing in Wireless Sensor Networks and its Challenges", *International Journal of Engineering and Advanced Technology* (*IJEAT*), ISSN: 2249 – 8958, Vol. 9 Issue1, pp. 4024-4027, Oct. 2019,

[10] Anil. G.L, J.L. Mazher Iqbal, "Implementation of Secure Energy Efficient Network Priority Routing (SEENPR) Protocol with Secure Key Management in WSN", *International Journal of Recent Technology and Engineering* (*IJRTE*), ISSN: 2277-3878, Vol. 8, Issue 2S11, pp. 3096-3103, Sep. 2019.

[11] Anand Nayyar, "Improvised Energy Efficient Routing Protocol based on Ant Colony Optimization (ACO) for Wireless Sensor Networks", *Ph.D. Thesis, Department of Computer Science Desh Bhagat University*, Mandi Gobindgar, Punjab, 2017.
[12] Musheer Vaquar, Sanjay Kumar Agarwal, "HETRP: High Energy Efficient Trustable Routing Protocol for Wireless Sensor Network International", *Journal of Innovative Technology and Exploring Engineering* (*IJITEE*), ISSN: 2278- 3075, Vol. 9 Issue 3, pp. 1034-1042, Jan. 2020.
[13] S. Ganesh and R. Amutha, "Efficient and Secure Routing Protocol for Wireless Sensor Networks through Optimal Power Control and Optimal Handoff-Based Recovery Mechanism", *Hindawi Publishing Corporation's Journal of Computer Networks and Communications*, Vol. 2012, Article ID 971685, 8 pages , 2012.
[14] Anil. G.L, J.L. Mazher Iqbal, "Implementation of Secure Energy Efficient Network Priority Routing (SEENPR) Protocol with Secure Key Management in WSN", *International Journal of Recent Technology and Engineering* (*IJRTE*), ISSN: 2277-3878, Vol. 8, Issue 2S11, pp. 3096 – 3103, Sep. 2019.
[15] Qu Y., Zheng G., Wu H., Ji B. & Ma H., "An Energy- Efficient Routing Protocol for Reliable Data Transmission in Wireless Body Area Networks", *Journal of Sensors, Basel, Switzerland)*, Vol. 19, No. 19, pp. 4238. 2019.
[16] Rajdip Pau & Banani Das, "A Survey on Energy Efficient Routing Techniques and Security Measures in Wireless Sensor Network", *Conf. Paper*.
[17] Muhammad Kamran Khan, Muhammad Shiraz , Kayhan Zrar Ghafoor, Suleman Khan, Ali Safaa Sadiq and Ghufran Ahmed, "EE-MRP: Energy-Efficient Multistage Routing Protocol for Wireless Sensor Networks", *Hindawi Wireless Communications and Mobile Computing*, Vol. 2018,
Article ID 6839671, 13 pages, 2018
[18] K. Nattar Kannan and B. Paramasivan, "Development of Energy-Efficient Routing Protocol in Wireless Sensor Networks Using Optimal Gradient Routing with On Demand Neighborhood Information", *Hindawi Publishing Corporation's International Journal of Distributed Sensor Networks*, Vol. 2014, Article ID 208023, 7 pages, 2014.
[19] Yogini Anant Patil, Rahul Gaikwad, "A Study on Enhanced Energy-Efficient and Reliable Routing for Mobile Wireless Sensor Networks with authentication", *International Journal of Innovative Research in Computer and Communication Engineering*, ISSN(Online): 2320-9801, ISSN (Print): 2320-9798, Vol. 5, Issue 1, pp. 259-263, Jan. 2017,
[20] R. Logeswari & V. Manimaran, "A Survey on Secure and Energy Efficient Routing in Wireless Sensor Networks", *International Journal of Latest Engineering Science* (*IJLES*) E-ISSN: 2581-6659, Vol. 3, IJLES pp. 9-20, Issue 1, Jan – Feb. 2020.
[21] Patale, Jayshri Prakash, et al. "A Systematic survey on Estimation of Electrical Vehicle." Journal of Electronics, Computer Networking and Applied Mathematics (JECNAM) ISSN: 2799-1156 3.01 (2023): 1-6.
[22] Makarand M. Jadhav, et al. "Painless Machine Learning Approach to Estimate Blood Glucose Level with Non-Invasive Devices." Artificial Intelligence, Internet of Things (IoT) and Smart Materials for Energy Applications. CRC Press, 2022. 83-100.
[23] Rahul, G. Ghodake, et al. "Microcontroller Based Drip Irrigation System." (2016): 109-115.
[24] Patale, Jayshri Prakash, et al. "Python Algorithm to Estimate Range of Electrical Vehicle." Telematique (2022): 7046-7059.
[25] Takale, Swapnil, et al. "DWT-PCA based Video Watermarking." Journal of Electronics, Computer Networking and Applied Mathematics (JECNAM) ISSN: 2799-1156 2.06 (2022): 1-7.
[26] Shinde, Rahul, et al. "Analysis of Biomedical Image‖." International Journal on Recent &

Innovative trend in technology (IJRITT) (2015).
[27] Mandwale, Amruta, et al. "Different Approaches For Implementation of Viterbi decoder." IEEE International Conference on Pervasive Computing (ICPC). 2015.
[28] Takale, Swapnil, et al. "Video Watermarking System." International Journal for Research in Applied Science & Engineering Technology (IJRASET) 10.
[29] Maske, Yogita, et al. "Development of BIOBOT System to Assist COVID Patient and Caretakers." European Journal of Molecular & Clinical Medicine 10.01 (2023): 2023.
[30] Gadade, Bhanudas, et al. "Automatic System for Car Health Monitoring." International Journal of Innovations in Engineering Research and Technology (2022): 57-62.
[31] Yogita Maske, Mr. A. B. Jagadale et al. "Implementation of BIOBOT System for COVID Patient and Caretakers Assistant Using IOT". International Journal of Information Technology &Amp; Computer Engineering (IJITC) ISSN : 2455-5290, vol. 2, no. 01, Jan. 2023, pp. 30-43, doi:10.55529/ijitc.21.30.43.
[32] Godse, A. P., et al. (2009)." Embedded Systems (First Edition). pp.(1-5).
[33] Birajadar, Ganesh, and Channappa Bhyri. "Comprehensive survey on EEG analysis for detecting brain disorders." Mukt Shabd Journal IX (VI) (2020): 2258-2262.
[34] P. B. Mane, et al. "High speed area efficient FPGA implementation of AES algorithm", International Journal of Reconfigurable and Embedded Systems (IJRES), Vol 7, Is. 3, 157-165
[35] Dhabliya, D., & Others. (2021). An Integrated Optimization Model for Plant Diseases Prediction with Machine Learning Model. Machine Learning Applications in Engineering Education and Management, 1(2), 21–26.
[36] Anupong, W., Yi-Chia, L., Jagdish, M., Kumar, R., Selvam, P. D., Saravanakumar, R., & Dhabliya, D. (n.d.). Sustainable Energy Technologies and Assessments.
[37] Birajadar, Ganesh, and Channappa Bhyri. " cap sleep disorder identification using EEG analysis" Eur. Chem. Bull. 2023, 12 (S3), 1709 – 29.
[38] A. O. Mulani, Watermarking and Cryptography Based Image Authentication on Reconfigurable Platform. Universitas Ahmad Dahlan, 2017.
[39] Akshata Kambale. et al., "HOME AUTOMATION USING GOOGLE ASSISTANT", UGC care approved journal, Vol 32 Issue 1, 2023
[40] Dr. K. S. L. Kazi, et al. "Effect of Rotation and Projection on Real Time Hand Gesture Recognition System for Human Computer Interaction", Journal of Gujrat Research Society, Volume 21 Issue 16, Dec 2019.
[41] Birajadar, Ganesh. "Epilepsy Identification using EEG signal monitoring." Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12.2 (2021): 2366-2371.
[42] R. A. Sawant, et al. "Automatic PCB Track Design Machine", International Journal of Innovative Science and Research Technology, Vol 7, Issue 9, Sept 22.
[43] Rutuja Abhangaro, et al. "DESIGN AND IMPLEMENTATION OF 8-BIT VEDIC MULTIPLIER", International Journal of Research Publications in Engineering and Technology (ISSN No: 2454-7875), March 2017.
[44] Mahesh Seth, et al. "Painless Machine learning approach to estimate blood glucose level of Non-Invasive device", Artificial Intelligence, Internet of Things (IoT) and Smart Materials for Energy Applications, 2022.