IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-4, Issue-6 E-ISSN: 2347-2693

Node Attestation for Reliable Communication in WSN

Ranjit Kaur [1*] and Khushboo Bansal [2]

[1*,2] Department of Computer Science and Engineering, Desh Bhagat University, Punjab, India

Received: May/12/2016 Revised: May/24/2016 Accepted: Jun/17/2016 Published: Jun/30/2016

Abstract: A wireless sensor network is a group of specialized transducers with a communications infrastructure for monitoring and recording conditions at diverse locations. In this paper various approaches were described that were used for WSN. Leach is used in wireless sensor network and multi-hop leach protocol is used for energy consumed in a single hop for defining energy consumed in a single hop .By receiving various protocols the conclusion occur that leach is best protocol for WSN**.**

Keywords**:** routing strategy, attestation algorithm, nodes

1. INTRODUCTION

1.1 Wireless Sensor Network

A wireless sensor network is a group of specialized transducers with a communications infrastructure for monitoring and recording conditions at diverse locations. Commonly monitored parameters are temperature, humidity, pressure, wind direction and speed, illumination intensity, vibration intensity, sound intensity, power-line voltage, chemical concentrations, pollutant levels and vital body functions.

Fig 1.1 Wireless Sensor Networks

In computer science and telecommunications, wireless sensor networks are an active research area with numerous workshops and conferences arranged each year, for example IPSN, Senses, and EWSN.

1.2 Parts of WSN [1-10]

1.2.1 Sensor Node: This is a core component of WSN. This node plays a multiple roles in WSN, such as simple sensing; data storage; routing; and data processing.

1.2.2 Clusters: Clusters are the organizational unit for WSNs. The dense nature of these networks requires the need for them to be broken down into clusters to simplify tasks such a communication.

1.2.3 Cluster heads: Cluster heads are the managing the cluster head. They often are needed to managing task in the cluster. These tasks include but are not limited to data-aggregation and organizing the communication schedule of a cluster.

1.2.4 Base Station: The base station is at the upper level of the hierarchical WSN. It provides the communication link between the sensor network and the end-user.

1.2.5 End User: The data in a sensor network can be used for a wide-range of applications. Therefore, a particular application may make use of the network data over the internet, using a PDA, or even a desktop computer.

1.3 Routing Protocols in WSN

We can reduce the energy consu7mption by using various techniques like data aggregation, clustering, data-centric methods, etc. The routing protocols can be classified as flat, hierarchical or location-based as follow:

1.3.1 Flat networks: In this network equal nodes are used. Hence each node plays the same role. This network has no logical hierarchy. It uses a flat addressing scheme. The example of flat network is Routing Information Protocol (RIP)

1.3.2 Hierarchical networks: The nodes are partitioned into a number of small groups called clusters. Each cluster has a cluster head (CH) which is the coordinator of other nodes. These CHs perform data aggregation so that energy inefficiency may be reduced. The cluster heads may change. The node which has the highest energy acts as the CH.

Hierarchical routing is an efficient way to lower energy consumption within a cluster. It has major advantages of scalability, energy efficiency, efficient bandwidth utilization, reduces channel contention and packet collisions. Low Power Adaptive Clustering Hierarchy (LEACH), Hybrid, Energy-Efficient Distributed Clustering (HEED), etc. are examples of hierarchical networks [20].

1.3.3 Location-based networks: In location-based clustering, the location of the sensor nodes plays a important role. Base station is used to send data to a particular location. In these protocols, the awareness of position of the sensor nodes is very significant to transfer the data to destinations. The distance between neighboring nodes can be estimated on the basis of incoming signal strengths. On the basis of location based protocol, if there is no activity then nodes should go to sleep to save energy. Location-Aided Routing (LAR) and the example of location based protocol Distance Routing Effect Algorithm for Mobility (DREAM).

2. REVIEW OF LITERATURE

Pushpendu Karet al [11] "Reliable and Efficient Data Acquisition in Wireless Sensor Networks in the Presence of Transfaulty Nodes" These effects result in loss of information in the radiation-affected area. To prevent information loss in WSN due to transfaulty behavior of sensor nodes, in the proposed scheme, we construct the network using sensor nodes having dual mode of communication-RF and acoustic. To get redundant coverage within a radiation affected area, all the sensor nodes in the area become activated and switch to the acoustic communication mode after detecting themselves to be affected by radiations. In-network data fusion is performed to get actual information from the redundant information received from the radiation-affected area. Simulation results exhibit that the proposed scheme, Re DAST, achieves better energy efficiency and reduced average end-to-end delay than sensor nodes having only acoustic mode of communication

Mitra, S. et al [12] "Energy aware fault tolerant framework in Wireless Sensor Network" Wireless Sensor Network, composed of tiny sensor devices and wireless network, is mainly responsible for any kind of ambience surveillance. Due to the peripheral atmosphere in which it is deployed, tiny sensors or the network might be too much fault prone. It is beneficial if and only if sensed values are fault free and it can traverse through fault free path. Thus it is necessary to monitor the network and the sensor nodes in regular interval to generate required result for application specific decision making. Network lifetime play the crucial role in order to monitor network health.

Deshpande, P. et al [13] "Techniques improving throughput of wireless sensor network: A survey" In wireless sensor networks, maintaining the higher throughput is the main concern. Wireless senor networks are basically formed with a few powerful base stations and a large number of resource-constrained sensor nodes. The wireless sensor network composed of n number of sensors or nodes, where each and every node is connected to one or several nodes or sensors. For providing low data rate for short coverage and long battery life, zig bee is used in wireless sensors network and ultimately zig bee nodes are used in wireless sensor network which are called as zig bee sensor nodes. Wireless sensor nodes of zig bee system basically build on two aspects of protocol stack that are IEEE 802.15.4 standard and zig bee protocol.

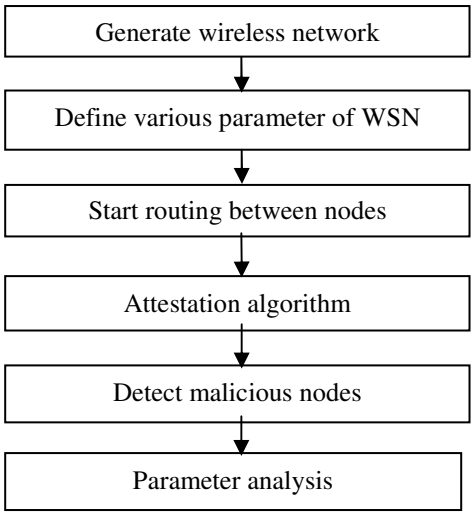
Makhdoom, I. et al [14] "A novel code attestation scheme against Sybil Attack in Wireless Sensor Networks" Wireless Sensor Networks (WSN) due to their distributed nature are vulnerable to various external and insider attacks. Classic cryptographic measures do protect against external attacks to some extent but they fail to defend against insider attacks involving node compromise. A compromised node can be used to launch various attacks of which Sybil Attack is the most prominent. In this paper we carryout a detailed review and analysis of various defenses proposed against Sybil Attack. We identify their strengths and weaknesses and also propose a novel One Way Code Attestation Protocol (OWCAP) for wireless sensors networks, which is an economical and a secure code attestation scheme that protects not only against Sybil Attack but also against majority of the insider attacks.

Krithiga, J et al [15] "Efficient Code Guard mechanism against pollution attacks in interflow Network coding" The study of Network coding and the impact of data pollution attacks is done in wireless network. The main focus is on pollution attacks and defenses in interflow network coding systems. While most of the prior work is on detecting and filtering polluted packets in interflow network coding systems. But we deal with interflow coding systems. An additional goal is to identify and eliminate the attacker nodes quickly between 500-1sec of attack. The Code Guard, a defense mechanism that combines proactive node attestation and reactive trace back identifies and eliminates the attacker nodes unequivocally. Analysis of Code Guard proved that it is always able to identify and isolate at least one attacker node on every occurrence of a pollution attack. Experimental demonstration shows that Code Guard is able to identify attacker nodes quickly and restore system throughput to a high level, even in the presence of many attacker nodes, thus preserving the performance of the underlying interflow network coding system.

Geetha, R. et al [16] "Fuzzy logic based compromised node detection and revocation in clustered wireless sensor

networks" Wireless sensor networks contain a large number of nodes which are unattended in nature where an adversary can physically capture and compromise the nodes and later inject a range of attacks with these compromised nodes. Researchers recently have proposed a number of compromise detection schemes in sensor networks. We propose a cluster based node compromise node detection and revocation scheme which reduces the limitations of the existing schemes. In this scheme the concept of Fuzzy logic is used to make a decision over the clusters whether they contain suspicious nodes. After identifying the suspected clusters the software attestation is performed against the nodes which lead to the identification and revocation of compromised nodes from the network. Our proposed scheme shows that it performs well in the presence of false positives and false negatives.

3. METHDOLOGY



4. RESULTS

WSN has been generated in network simulator for simulation of purposed work in the network. So that data aggregation can be enhanced in the network. in the purposed work network simulation parameters have been initialized for deployment of sensor network over the sensing environment so that network can be used for capturing information from sensing environment. In the sensing environment message has been broadcasted by the node for data transmission over the network to find route so that data can be transmitted to various cluster nodes or data aggregation points available in the network. Simulation setup has been done and various network parameters have been analyzed for performance evaluation of purposed work.

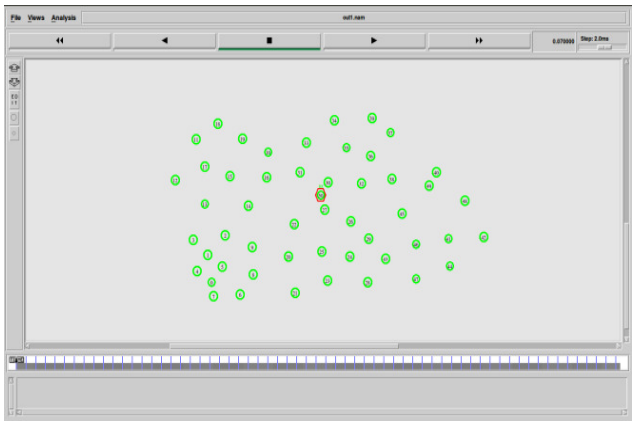


Fig 5.1: Initialization of nodes

This scenario is used to represent the initialization of nodes. Numbers of nodes are 50 out of which node 50 is called base station.

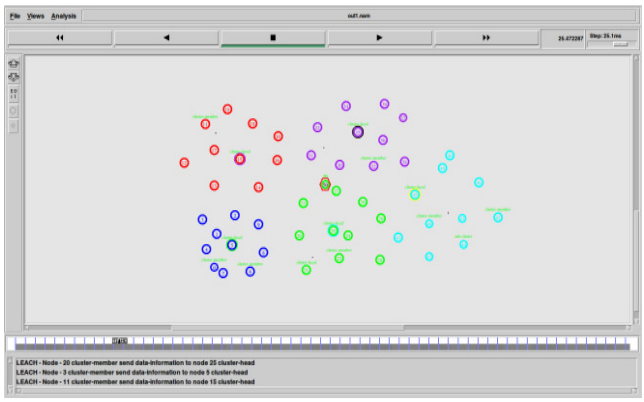


Fig 5.2: Initialization of cluster head & base station

This scenario is use to represent the Cluster Heads. Number of cluster heads are 5. Base station (node 50) takes the back up of all the data.

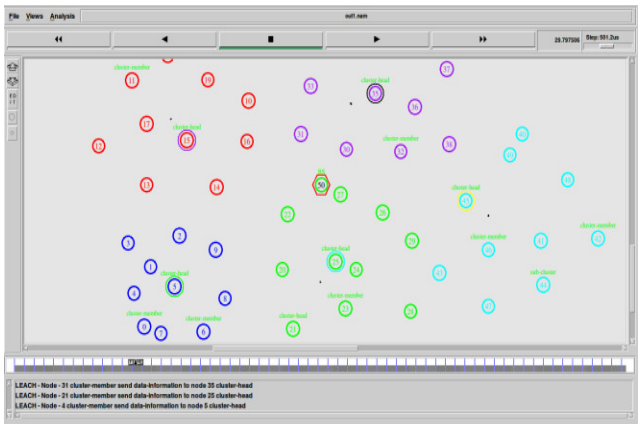


Fig 5.3: Transmission of data

This scenario is use to represent the transmission of data. All the members of cluster send data to the cluster head.

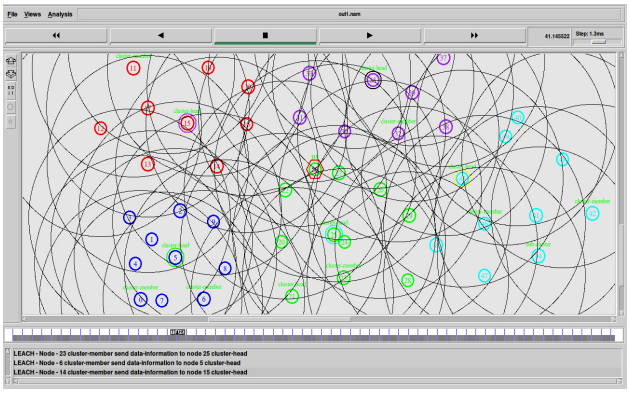


Fig 5.4: Routing

This scenario is use to represent the routings between the nodes.

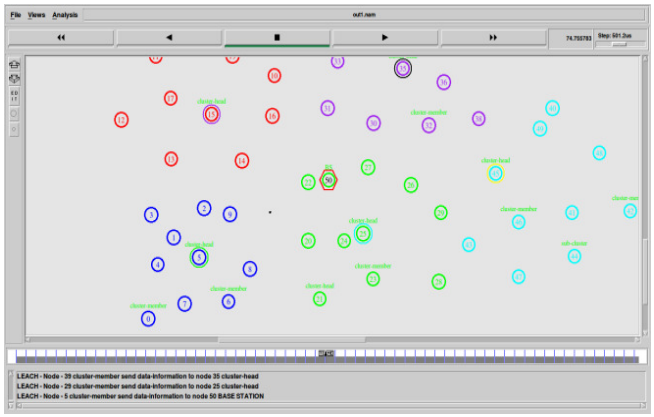


Fig 5.5: Transmission b/w cluster heads & base station

This scenario is use to represent the transmission of data between the cluster heads and the base station. All the cluster heads send data to the base station i.e node 50.

Fig 5.6 Packet Delivery Ratio

In this X-axis represent the time and Y-axis represent the bytes sent over the network. This figure is used to represent the Packet Delivery Ratio. Packet Delivery Ratio is defined as the number of packets delivers with respect to time.

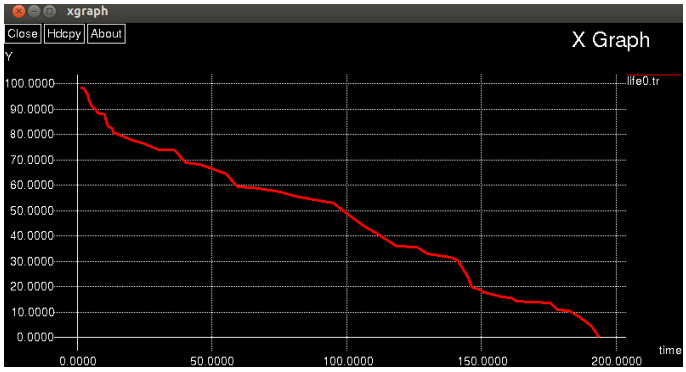


Fig 5.7 Life time

This figure is use to represent the Lifetime of a node. Lifetime is defined as the total time in which node can survive without any disturbance.

This figure is use to represent the throughput. Throughput is defined as the number of packets delivered successfully in a particular interval of time over the network.

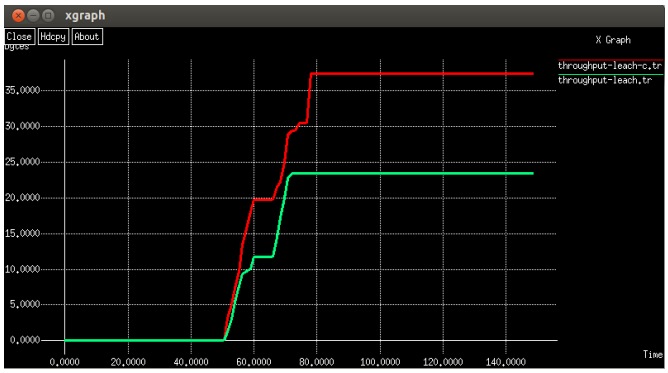


Fig 5.8 Packet Delay

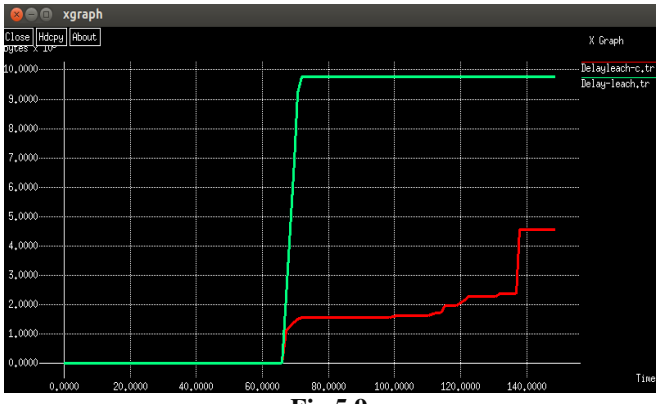


Fig 5.9

This figure is use to represent the Packet Delay. Packet Delay is defined as the Delay between packets during transmission.

5. CONCLUSION & FUTURE SCOP

A wireless sensor network is a gathering of specific transducers with a corresponding foundation for observing and recording conditions at diverse areas. Generally checked parameters are temperature, humidity, weight, wind direction and velocity, enlightenment force, vibration power, sound force, force line voltage, substance focuses, pollutant and basic body capacities. WSN is used for sensing the information from environment. These sensors have sensor range and sense the information from particular area. Various protocols were purposed for proper utilization of energy in wireless network. Leach was a basic protocol that was used as energy model in WSN. In this paper various approaches were described that were used for WSN. Leach is used in wireless sensor network and multi-hop leach protocol is used for energy consumed in a single hop for defining energy consumed in a single hop .By receiving various protocols the conclusion occur that leach is best protocol for WSN**.**

REFRENCES

[1] Xinyu Jin "Unpredictable Software-based Attestation Solution for node compromise detection in mobile WSN" *IEEE Globecom Workshops*, pp.2059 – 2064,2010.

[2] Tamer AbuHmed "Software-Based Remote Code Attestation in Wireless Sensor Network" *IEEE Global Telecommunications Conference*, pp. 1 – 8, 2009.

[3] Po-Hung Yang "Memory Attestation of Wireless Sensor Nodes by Trusted Local Agents*" IEEE* ,pp. 82 – 89,2015.

[4] Ahmad Salehi S. "Detection of Sinkhole Attack in Wireless Sensor Networks", *IEEE International Conference on Space Science and Communication*, 2013, pp. 361-365.

[5] A. Vijayalakshmi., "Mobile Agent Middleware Security for Wireless Sensor Networks" *IEEE International Conference on Communication and Signal Processing*, 2014, pp. 1669-1673.

[6] Van dana B. Salve, "AODV Based Secure Routing Algorithm against Sinkhole Attack in Wirelesses Sensor Networks*", IEEE International Conference on Electrical, Computer and Communication Technologies*, 2015, pp. 1 – 7.

[7] Mohamed Guerroumi "Intrusion detection system against SinkHole attack in wireless sensor networks with mobile sink"*IEEE International Conference on Information Technology*, 2015, pp. 307- 313.

[8] Sheela, D. "A non cryptographic method of sink hole attack detection in wireless sensor networks*" IEEE International Conference on Information Technology*, 2011, pp. 527 – 532.

[9] Guerroumi, M., "Intrusion Detection System against Sink Hole Attack in Wireless Sensor Networks with Mobile Sink" *IEEE International Conference on Information Technology - New Generations*, 2015, pp. 307 – 313.

[10] Varshney, K.K. "Performance analysis of malicious nodes in IEEE 802.15.4 based wireless sensor network" *IEEE International Conference on Information Communication and Embedded Systems,* 2014, pp. 1 – 5.

[11] Ritwik Banerjee "Energy efficient routing and bypassing energy-hole through mobile sink in WSN" *IEEE Conf. on Computer Communication and Informatics (ICCCI*), 2014, pp. 1 – 6.

[12] Babar Nazir "Mobile Sink based Routing Protocol (MSRP) for Prolonging Network Lifetime in Clustered Wireless Sensor Network" *IEEE Conf. on Computer Applications and Industrial Electronics (ICCAIE*), 2010, pp. 624 – 629.

[13] Pushpendu Karet "Reliable and Efficient Data Acquisition in Wireless Sensor Networks in the Presence of Transfaulty Nodes" *IEEE Conf. on IEEE Transactions on Network and Service Management*, 2016, pp. 99 – 112.

[14] Mitra, S "Energy aware fault tolerant framework in Wireless Sensor Network" *IEEE Conf. on Applications and Innovations in Mobile Computing* (AIMoC),2014,pp- 139 – 145.

[15] Deshpande, P. "Techniques improving throughput of wireless sensor network: A surveogies y" *IEEE Conf. on Circuit, Power and Computing Technol (ICCPCT)*,2015,pp- 1 – 5.

[16] Makhdoom, I. "A novel code attestation scheme against Sybil Attack in Wireless Sensor Networks*" IEEE Conf. on Software Engineering Conference (NSEC*), 2014 ,pp- 1 – 6.

[17] Krithiga, J "Efficient Code Guard mechanism against pollution attacks in interflow Network coding*" IEEE Conf. on Communications and Signal Processing (ICCSP), 2014,pp-* 1384 – 1388.

[18] Geetha, R. "Fuzzy logic based compromised node detection and revocation in clustered wireless sensor networks*" IEEE Conf. on Information Communication and Embedded Systems (ICICES),2014,pp-* 1 – 6.

[19] Yong-Sik Choi, "A study on sensor nodes attestation protocol in a WireleCACTss Sensor Network*", IEEE Conf. on Advanced Communication Technology (I), 2010,* pp. 1738-9445.

[20] Yuling Lei "The Research of Coverage Problems in Wireless Sensor Network", *IEEE Conf. on Wireless Networks and Information Systems*, 2009, pp 31 – 34.