A Review of Power Optimization and Attack Analysis in Wireless Sensor Network

Ritu Vishwakarma
M.Tech Scholar, Department of CSE
VITS, Bhopal, India
E-mail- rituvishwakarma15@gmail.com

Sumit Sharma
Assistant Professor, Department of CSE
VITS, Bhopal India
E-mail- sumit_sharma782022@gmail.com

ABSTRACT
In current scenario ZigBee wireless sensor network suffered from distribution of power and route cost for the selection of root tree node and communicating node. The utilization of power factor in sensor network is limited due to this reason most of authors used the process of energy consumption for the increasing the life of network. The power supply process of wireless sensor network is fixed type. The process of power used battery. In the process of improvement of ZTR protocol one protocol are available such are called as STR protocol. Basically STR protocol is a combination of two different routing protocols for the processing of energy saving mode and cost. The STR protocol design on the principle of AODV and tree based routing mode selection based on limited power threshold factor. The research gap between ZTR and STR is sharing of information for the selection of tree node process. During the cluster node selection more power is consumed. Now reduction of this power effect used reference node selection mode for the selection of tree head and data transmission for the communicating node. In this paper we focus on the brief literature survey work for a wireless sensor network and their techniques for security concerned.

Keywords: -STR, ZTR, AODV, Attack, LEACH.

.

INTRODUCTION

A wireless sensor network (WSN) is a group of sensor nodes which are deployed in a field to monitor physical conditions autonomously. WSNs can measure various physical conditions like sound, temperature, pressure, humidity, load, speed etc. After sensing the data sensor nodes pass this information to a base station or sink following a particular routing pattern. The number of sensor nodes in a WSN can vary from a few to hundreds or thousands in numbers depending on the application. A sensor node consists of many components, a microprocessor or a microcontroller to control the operation of node, a radio transceiver to transmit and receive information, an ADC converter to convert analog information to digital and vice versa and a power source [2]. In wireless sensor network, the network structure can be divided into three main protocols; flat-based routing, hierarchical-based routing and location-based routing. Flat-based routing usually involves sensor nodes that has equal roles that works together to perform sensing task. In this protocol, data centric routing and attribute-based naming are used in most routing protocols in order to create a more efficient communication. Hierarchical-based routing provides more efficient routing where the sensor nodes are usually clustered and led by cluster heads which can process and aggregate more with the sensor nodes senses data [1].

WSNs are currently being employed in a variety of domains ranging from commercial, industrial, environmental, and healthcare to military applications to monitor data that would be difficult or expensive to capture using wired sensors [10]. Such as Aircraft Monitoring, Ecological Habit Monitoring, Geological Monitoring, Wireless Biomedical Sensor Networks, Event Detection, Multimodal Node Localization, Collaborative Self-Localization, Traffic Monitoring and Target Tracking.

WSN face unique set of security challenges [20]. WSN not only need confidentiality, authentication and data integrity, but trust as well. Nodes deploy in hostile environments where attackers can physically tamper with nodes. Nodes must be produced cheaply to be cost-effective; therefore nodes are severely underpowered compared to laptop class attackers. Below is an overview of potential attacks.

HELLO FLOOD: The hello flood attacks nodes using a powerful transmitter by advertising routes to the gateway. Nodes receiving the message see the attacker as a nearby node with a short route to the gateway, but the attacker is actually outside the transmission range of most nodes. Neighboring nodes become confused when data sent to the advertised route disappear. The hello flood also works with replayed messages [11].

SPOOFING/MESSAGE ALTERING: Spoofed and altered messages are simple attacks that modify messages to confuse message recipients. Altered messages can spread false routing information to cause bad routing decisions. Bad routing in WSN translates to longer paths and wasted energy. This attack can be defeated by an integrity check such a Message Authentication Code (MAC) [12].

REPLAY ATTACK: replay attack captures and retransmits a message. Replay attacks are unaffected by encryption. A nonce or timestamp is necessary to counter replayed messages. Timestamps are preferred by WSN because they require fewer messages.

WARMHOLE: A wormhole is a coordinated attack between two attackers capable of communicating through other means than the normal communication. An example would be two computers at opposite ends of the network, communicating through a different frequency. The attackers share information only available to the other node. The attackers then advertise a better route than the ones available, causing neighboring nodes to use the attacker as an intermediary hop. This attack sets-up other attacks such as selective forwarding.

SELECTIVE FORWARDING: Selective Forwarding works when an attacking node places itself in the routing path of another node. The attacker then chooses which packets to forward to the next hop and which packets to drop. The most basic selective forwarding attack is a sinkhole. A sinkhole drops all arriving packets. Often routing protocols detect sinkholes as broken links and attempt to avoid the link.

The rest of this paper is organized as follows. In Section II describe about the literature review, and in The Section III shows the problem formulation and states the problem in brief and finally section IV discusses conclusion and future work.

III RELATED WORK

This section gives an extensive literature survey on the existing routing protocol for increase the efficiency of energy used in a communication and also gives the secured communication and increase the range of communication area. The aim of this survey to find the work guidance of efficient reliable routing protocol. We study various research paper form IEEE, ACM, Elsevier and International journal and know about energy efficiency routing protocol and secured routing protocol in mobile wireless sensor network. All methodology and processing are not described here. But some related work in the field of wireless sensor network security and power reduction discuss by their respective title and their contribution of work. A lot of work has been done on proposing solutions to the fundamental issues generated when integrating wireless sensor network.

Siti Ummi Masruroh, Khadijah Utami Sabran Et al. [1] Here they propose an algorithm design based on what wireless sensor network is initially created for. The design of the algorithm will focus on the sensor network's quality of service (QoS), emergency awareness, and energy efficiency. The designed algorithm is intended for wireless sensor networks that needs a period and event-driven approach and can adapt to the situation the sensor faces. Their motivation is to expand the solution of problems found in routing protocol specifically in the quality of service issue. In terms of quality of service, data must be delivered in an accurate amount of time for it to be useful. However, with a better delivery of service in data, the energy consumption will inevitably increase and shorten the lifetime of network. A dynamic routing protocol must be able to offer a trade-off between the two, thus a lot of routing protocol now have been designed to be energy-aware.

Jyoti Singh, Bhanu Pratap Singh, Subhadra Shaw Et al. [2] This paper proposes a new routing strategy based on hierarchical routing protocol LEACH where clusters are refreshed periodically based on residual energy and distance. Re-clustering distributes the workload among different nodes and in turn enhances the network lifetime by rotating the cluster head. The sensor nodes remain in active state only during its transmission slot. Rest of the time it remains in sleep state to save energy. LEACH, MOD-LEACH and the proposed protocol are simulated in MATLAB. The result shows that our proposed algorithm performs better than the LEACH and also MOD-LEACH protocol in terms of network lifetime. The proposed algorithm also gives more throughput than LEACH.

Vaishali Jain, Nayyar Ahmed Khan Et al. [3] This paper has been concentrated on the performance analysis of the two most prominent data centric protocols, Directed Diffusion and SPIN routing protocol. The performance analysis are examined using NS-2 which is the main network simulator, NAM (Network Animator), TCL (Tool Command Language), A WI((post processing script) and were compared in terms of performance parameters like End-to-End Delay, Throughput, Control Overhead and Packet Delivery Ratio (PDR). The research work demonstrated here is established by results based on performance analysis of DDIFF and SPIN routing protocol. It has been discovered that under all four parameter considering static as well as mobile environment, DDIFF performs better than SPIN routing protocol.

Young-Duk Kim,Soon Kwon,Woo Young Jung, Dongkyun Kim Et al. [4] In this paper, They propose an emergency adaptive communication protocol, which treats the data packet in a discriminatory manner by investigating whether it is emergency or not. Hence, the proposed protocol defines an emergency factor for each data packet and exploits it for both route establishment and channel access procedures. In route establishment, the proposed protocol chooses a route with low delay and high reliability among the candidates by periodic calculation of emergency factor. Then, it dynamically adjusts back-off parameters before participating in the channel contention among the neighbors.

Keerti Naregal, Anand Gudnavar Et al. [5] In this work the classical cluster routing protocol LEACH and improvement of LEACH(LEACH-E) are analyzed and improved (LEACH-EX). In LEACH-E energy depletion of nodes is balanced by two methods; first by considering the current energy of nodes when electing them as cluster heads, another is by limiting the number of nodes in each cluster. In LEACH-EX the threshold formula for election of cluster heads is simplified and simulation results show the effectiveness of the formula (LEACH-EX) and prove that LEACH-EX is much better than LEACH and LEACH-E in energy consumption and lifetime of network. Sensor networks can contain hundreds or thousands of sensing nodes. It is desirable to make these nodes as cheap and energy-efficient as possible and rely on their large numbers to obtain high quality results.

Samer A. B. Awwad, Chee K. Ng, Nor K. Noordin Et al. [6] In this paper, they propose adaptive Time Division Multiple

Access (TDMA) scheduling and round free cluster head protocol called Cluster Based Routing (CBR) protocol for Mobile Nodes in Wireless Sensor Network (CBR Mobile-WSN). In this protocol the cluster head receive data from not only its member during the TDMA allocated time slot but also other sensor nodes that just enter the cluster when it has free time slots, each cluster head takes turn to be the free cluster head in the network. CBR Mobile-WSN change TDMA scheduling adaptively according to traffic and mobility characteristics. The proposed protocol sends data to cluster heads in an efficient manner based on received signal strength. The performance of proposed CBR Mobile-WSN protocol is evaluated using MATLAB and it has been observed that the proposed protocol reduces the packet loss by 25% compared to LEACH-Mobile protocol.

Adamu Murtala Zungeru, Li-Minn Ang, Kah Phooi Seng Et al. [9] In this paper author presents a comprehensive survey and comparison of routing protocols in WSNs. The first part of the paper surveys state-of-the-art routing protocols in WSNs from classical routing protocols to swarm intelligence based protocols. The routing protocols are categorized based on their computational complexity, network structure, energy efficiency and path establishment. The second part of the paper presents a comparison of a representative number of classical and swarm based protocols. Comparing routing protocols in WSNs is currently a very challenging task for protocol designers. Often, much time is required to re-create and re-simulate algorithms from descriptions in published papers to perform the comparison. Compounding the difficulty is that some simulation parameters and performance metrics may not be mentioned.

III PROBLEM STATEMENT

The purpose of this paper is to minimize the power consumption of wireless sensor network during the selection of tree node during the process of routing. Wireless sensor nodes which are battery operated are used for detecting and collecting information from the areas where there is very little scope for manual handling to recharge or change batteries. These sensing nodes collect the information and pass them on to the network towards the sink for further actions. For a better functioning and a longer lifetime for a sensing node within the network, we need to consider its energy consumption as a major factor of concern. In the process of survey found that some protocol are very efficient such as ZTR and STR. The shortcut tree routing protocol is version of AODV protocol. Wireless sensor networks consist of a number of sensing nodes which are distributed in a wide area. They sense an event occurring in the environment and these sensing nodes are distributed or placed according to the requirements of the application.

- The base station (sink), which collects data from other nodes, interacts with a user (someone interested in monitoring the activity). Data can be collected in many ways from a sensing node to a sink node like using hopping techniques or transmitting data at certain frequencies. Sinks have more advanced features than sensing nodes in terms of data transmissions and processing capabilities, memory size and energy reserves. There can be multiple sinks for a network so that there is no single point of failure.
- Energy dissipation is a major factor in WSNs during communication among the nodes. Energy should be saved, so that the batteries do not get depleted or drained quickly as these are not easily replaceable in applications such as surveillance.
- Quality of service ensures the effective communication within the given or bounded delay time. Protocols should check for network stability, redundant data should be transmitted over the network for any type of traffic distribution. It also needs to maintain certain resource limiting factors, such as bandwidth, memory buffer size and processing capabilities.
- The transmission mode plays an important role in WSNs. Nodes can take single-hop or multi-hop depending upon the type of network topology chosen for communicating or transmitting data to other nodes within the network.
- The sensor nodes can be mobile or static depending on the application. In surveillance applications, sensor nodes are placed in unattended areas so it should be self-organizing and self-creating.
- The STR protocol gives the efficient routing protocol but it is faced a problem of multi-request join communication.

The consumption of power is increase due to large number of sensor node in active mode.

IV CONCLUSION AND FUTURE WORK

This paper provides minimization of energy consumption and minimization of routing cost for ZigBee wireless sensor network in concern of power consumption and life time of network. The proposed models give a better energy utilization factor for wireless sensor network. The proposed model ISTR implies in two section one is reference node and another node as Tree. The node end request for communication for next node in installed location of tree node. ISTR is a hybrid model of very famous reference node model and STR protocol for energy saving and minimum route cost for communication in wireless sensor network. Basically ISTR work as a route filter, because in modern trend traffic apply by the flooding a power that power is consumed by sensor node. Flooding blocks a provided bandwidth of communication and our network are jam without generation of any interference attack and jamming attack. So we design strong filter for unknown control request power on the time of node mobility. In this process our methods generate a link for connecting a mobile node with their respective speed and all nodes connect our base node, basically base node is a nothing, this is a control section of ISTR and maintains all links from mobile node. Link of synchronization provided by clock. Clock maintains network ability for all nodes during communication. If unknown mobile node sends a request to any node, node not reply, node transfer that message to chock section chock scan their power and find this is normal or abnormal and take action for blocking and generating a security alarm for all node.

The proposed model ISTR estimate communication power loss rate of vehicle ad-hoc network with data powers, form Experimental results we can conclude:
1. Power loss rate of WSNs is affected by a number of factors, such as flooding of control message protocol.
2. ISTR is an accurate model to estimate power loss rate and route cost, due to its stable and clear filtration process, its PDF is more accurate, and maximum a posteriori algorithm is less complexity and share good real-time performance.
ISTR can estimate the communication package loss rate with a smaller error, and can track the tiny change about it. It can be used to grasp the overall characteristics of the communication, support the data transmission control and routing algorithms in network protocol. The diversity of network and service oriented traffic in wireless ZigBee sensor network further explored our research work in term of calculation of power node assignment, for the process as base node for controlling a message request of all mobile sensor node in communicating network. The filtration process used huge amount of power for the process of selection, now need some extra memory segment for the process of reference node. Now exploding of this works and optimized the process of reference node allocation and reduces the capacity of memory for the expanding of power allocation.

REFERENCES

[1] Siti Ummi Masruroh, Khadijah Utami Sabran "Emergency-Aware and QoS Based Routing Protocol in Wireless Sensor Network" IEEE, 2014. Pp 47-51.

[2] Jyoti Singh, Bhanu Pratap Singh, Subhadra Shaw "A New LEACH-based Routing Protocol for Energy Optimization in Wireless Sensor Network" Conference on Computer and Communication Technology, IEEE, 2014. Pp 181-186.

[3] Vaishali Jain, Nayyar Ahmed Khan "Simulation Analysis of Directed Diffusion and SPIN Routing Protocol in Wireless Sensor Network" IEEE, 2014. Pp 1-6.

[4] Young-Duk Kim,Soon Kwon,Woo Young Jung, Dongkyun Kim "An Emergency Adaptive Communication Protocol for Driver Health Monitoring in WSN Based Vehicular Environments" International Journal of Distributed Sensor Networks, 2015. Pp 1-9.

[5] Keerti Naregal, and Anand Gudnavar "Improved Cluster Routing Protocol for Wireless Sensor Network through Simplification" 18th Annual International Conference on Advanced Computing and Communications, IEEE, 2012. Pp 1-3.

[6] Samer A. B. Awwad, Chee K. Ng, Nor K. Noordin, Mohd. Fadlee A. Rasid "Cluster Based Routing Protocol for Mobile Nodes in Wireless Sensor Network" IEEE, 2009. Pp 233-242.

[7] Hyunsook Kim "An Efficient Clustering Scheme for Data Aggregation Considering Mobility in Mobile Wireless Sensor Networks" International Journal of Control and Automation, Vol-6, 2013. Pp 221-234.

[8] Jianli Wang, Laibo Zheng, Li Zhao, Dan Tian "LEACH-Based Security Routing Protocol for WSNs" Springer, Vol-2, 2012. Pp 253-258.

[9] Adamu Murtala Zungeru, Li-Minn Ang, Kah Phooi Seng "Classical and swarm intelligence based routing protocols for wireless sensor networks: A survey and comparison" Journal of Network and Computer Applications, Elsevier, 2012. Pp 1508-1536.

[10] Aly Mohamed El-Semary, Mohamed Mostafa Abdel-Azim "New Trends in Secure Routing Protocols for Wireless Sensor Networks" International Journal of Distributed Sensor Networks, 2013. Pp 1-16.

[11] Jiliang Zhou "Efficient and Secure Routing Protocol Based on Encryption and Authentication for Wireless Sensor Networks" International Journal of Distributed Sensor Networks, 2013. Pp 1-18.

[12] D. Mahmood, N. Javaid, S. Mahmood, S. Qureshi, A. M. Memon, T. Zaman "MODLEACH: A Variant of LEACH for WSNs" 2013. Pp 1-6.

[13] Dervis Karaboga, Selcuk Okdem, Celal Ozturk "Cluster based wireless sensor network routing using artificial bee colony algorithm" Springer, 2012. Pp 847-860.

[14] W. Heinzelman, A. Chandrakasan, H. Balakrishnan "Energy-efficient communication protocol for wireless micro sensor networks" presented at the 33rd Hawaii Int. Conf. on System Sciences, January 2000.

[15] Zeenat Rehena, Sarbani Roy, Nandini Mukherjee "A Modified SPIN for Wireless Sensor Networks", IEEE, 2011. Pp 234-238.

[16] N. NARASIMHA DATTA, K. GOPINATH "A survey of routing algorithms for wireless sensor networks" Journal of Indian Institute of Science, 2006. Pp 569-598.

[17] Radia Perlman "Interconnections: Bridges, Routers, Switches, and Internetworking protocols" Second edition, Addison-Wesley (2000).

[18] Joanna Kulik, Wendi Heinzelman, Hari Balakrishnan "Negotiation-based protocols for disseminating information in wireless sensor networks" Wireless Networks, 2002. Pp 169–185.

[19] Baruch Awerbuch, David Holmer, Herbert Rubens, Kirk Chang, I. J. Wang "The Pulse protocol: sensor network routing and power saving" Military Communications Conference, 2004.

[20] Sami, S., Al-Wakeel , S., Al-Swailem, S.A. "PRSA: A Path Redundancy Based Security Algorithm for Wireless Sensor Network" IEEE WNC 2007 Proceedings, 2007.