INTERNATIONAL JOURNAL OF TECHNOLOGY AND COMPUTING (IJTC)
ISSN-2455-099X,
Volume 3, Issue 2 February 2017

To Maintain the Privacy in Moveable Sink to Prevent Active and Passive Attacks

Satish Kumar[1], Anil Bajaj[2], Anoop Kumar[3]

[123]Lovely Professional University Jalandhar, Punjab

Abstract: Wireless Sensor Networks (WSN) consists of large number sensor nodes. Wireless sensor nodes are generally deployed in the far places like forests deserts and used to sense the network conditions like temperature pressure etc. In such far places it is very difficult to recharge or replace the battery of the sensor node. The sensor nodes are battery powered devices, they communicate over a wireless medium and consumes energy during data transmission. The various types of active and passive attacks are possible in routing the data from source to sink. In this paper, we propose new technique to prevent these attacks. The mobile sinks is been deployed in the network which collect data from the sensor node and deliver data to fixed base station. In the proposed technique, the data privacy is ensured in the mobile sink.

Keywords: WSN, Mobile Sinks, Sensor node, Query, battery

I. INTRODUCTION

The wireless sensor network consists of large number of sensor nodes spread over the specific area where we want to sense the environment conditions like temperature, pressure, motion etc. The wireless sensor nodes consist of the power management module, sensor, processor and transreceiver. Sink is used to inject queries in to sensor field and sensor nodes are used to sense the event which is occurred in to field and give responds of that query. The data collected by the sensor nodes are send to the sink, sink is the like the base station which broadcast the data collected by the sensor nodes to the internet. Sensor node consists of four units which are as sensing unit, processing unit, Transreceiver unit and power management unit. Sensor unit consists sensor which is used to sense the changes in the environment, processing unit consists ADC which convert analog signal to digital signal and storage, and transreceiver unit consists transmitter which is used to transfer the data to next node. These three units are connected with power unit.

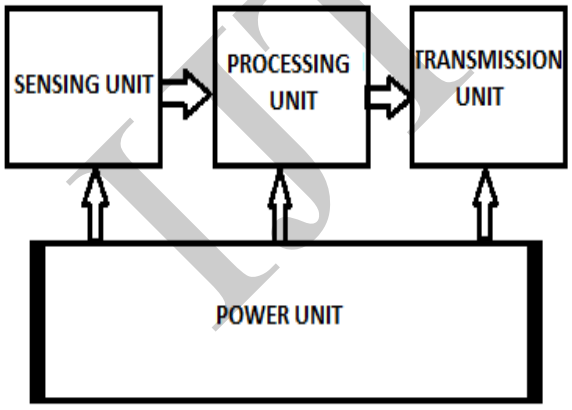

Fig1: Architecture of Sensor Node

As, shown in the figure power management module interact with the processor, sensing unit and with the Timing sync module. The sensor nodes communicate with the sink through the radio waves without use of any wires. If the node is not able to communicate with other through direct link, i.e. they are out of coverage area of each other, the data can be send to the other node by using the nodes in between them. All the sensor nodes are battery driven devices so the power management unit is very important issue in the wireless sensor network. The sensor nodes are communicate through a wireless medium like radio frequencies, infrared or any other medium, which is having no wired connection. Node gathers the data and transfer to as sink. The sink may connect to the outside world through internet. Sink collects the data from SN, and transfer to the user who requested it. The sink may also be an individual user who needs the desired information. The main problem in WSN is limited battery life of sensor nodes. Data transmissions consume battery power so any optimization in these networks should focus on optimizing energy consumption. For communication the network is flooded with the route request packets by the source node, every node responded back to the source node with route reply packet .The source node select the shortest path ,shortest path means the path which is having the minimum number of hops. In such scenario the active and passive attacks are possible. Attacks on ad hoc wireless networks can be classified as passive and active attacks, depending on whether the normal operation of the network is disrupted or not.

- **Passive attacks:** A passive attack does not disrupt the normal operation of the network; the attacker spoof the data exchanged in the network without altering it. Here the requirement of confidentiality gets violated.
- **Active attacks:** An active attack attempts to alter or destroy the data being exchanged in the network there by disrupting the normal functioning of the network. Active attacks can be internal or external. External attacks are carried out by that do not belong to the network. Internal attacks are from compromised nodes that are part of the network. Impersonation, modification, fabrication, and replay of packets.

To prevent these attacks new technique is proposed which is based on the sink movement. The mobile sinks are deployed in the sensor network. The mobile sinks collect data from the sensor nodes and deliver the data to fixed base station. To ensure data privacy in mobile sink new technique is been proposed in this paper.

II. LITERATURE REVIEW

Many techniques have been explored for the optimization of energy usage in wireless sensor networks. Routing is one of these areas in which attempts for efficient utilization of energy have been made. With help of efficient routing the best path from source to sink is chosen which reduce the traffic from network and increase the overall lifetime of network [1].

In WSN sensor nodes deployed densely and uniformly in the sensing field, a mobile sink injected Query packet by the mobile sink and routed to the specific area moving through the sensing field. Then the corresponding Response packet is returned to the mobile sink via multi-hop communication. Due to the mobility of the sink, the Query and Response should have different routes which reduce the collision and traffic and power consumption [2]. Wireless sensor networks consist of large number of sensor nodes which collected information from different environmental phenomena and sending base station which is called Sink. The sensors are having some faults like maintaining the network in proper functionality. In this paper the proposed method for recovering lost packets by caching data in some of network nodes which is a combination of Extended NAC and Active Caching (AC) methods and we call it New Active Caching (NAC) [3].

Due to the limited energy resource, energy efficient operation of sensor nodes is a key issue in wireless sensor networks. In proposed cooperative caching scheme for wireless sensor networks, one-hop neighbors of a sensor node form a cooperative cache zone and share the cached data with each other. It ensures sharing of data among various nodes reduces the number of communications over the wireless channels and thus enhances the overall lifetime of a wireless sensor network [4].

For improving WSN's energy efficiency that already uses an energy efficient data routing protocol the proposed improvements are (i) data negotiation in which active sensor sends its sensed data only when the data changes, (ii) development of data change expectancy in which a sensor develops the expectancy of when its sensed data might change, and (iii) data vanishing, duplicate sensed data from multiple sensors are discarded while routed to the base station [5]. The battery resource of the sensor nodes should be managed efficiently, to increase network lifetime in wireless sensor networks, multiple sink nodes should be deployed with time constraint that states the minimum required operational time for the sensor network which increase the manageability and reduce the energy consumption of each node [6]. Satoshi Kurosawa et al [9] proposed the solution emphasis on the dynamically changing conditions of ad hoc networks. In AODV, the destination sequence is used to determine the freshness of the routing information contained in the message from originating node. The attacker must generate its RREP with the destination sequence number greater than the destination sequence number of the destination node. It is possible to for the attacker to find the destination sequence number from the RREQ packet. But if other nodes attempts to construct the route to the destination node other than the source node, then the destination node's sequence number will be significantly different from the current destination sequence number**.**

III. NEW PROPOSED TECHNIQUE

In Wireless Sensor Network sink injects the query into the Network and sensor nodes responds to the query and the traffic depends on number of queries generated per mean time [7]. If sensor node having information about query then it replies to sink otherwise it floods the query to the other nodes. The sensor node will reply to the sink node through some routing protocol. In such scenario various type of active and passive attacks are possible. In the proposed technique to prevent attacks mobile sinks have been deployed in the network which is responsible for collecting and delivering the data to fixed base station. To ensure the data privacy in mobile sink the algorithm is proposed which is illustrated in figure2.

1. The sensor network is deployed with the finite number of mobile nodes
2. The sensor nodes sense the data
3. In the network main and sub sinks have been deployed
4. Sub sinks has the capability to move from one location to other location
5. The mobile sink store (coordinate information of fixed base station XOR password of fixed base station)
6. To maintain data privacy in mobile sinks following steps have been followed
   - The sensor nodes sense the environmental data
   - The mobile sink go to the particular location and collect the sensed data
   - The mobile sink go to fixed base station and deliver the collected data

   If ((coordinate information)XOR(fixed base station password) of mobile sink== information presented by fixed station)
   {
   Mobile sink deliver data to fixed base station
   }
   Else
   {
   Mobile sink don't deliver data to fixed station
   }

Fig 2: Proposed Algorithm

IV. RESULTS AND DISCUSSION

As, illustrated in figure 3. The comparison graph of delay between the existing techniques and new proposed techniques is shown. The red line shows the delay in previous techniques and green line shows the delay in new technique.

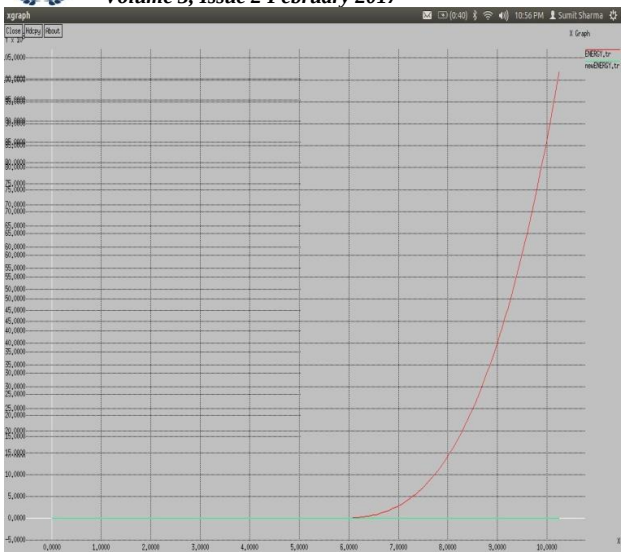

Fig3: Comparison graphs of Delay

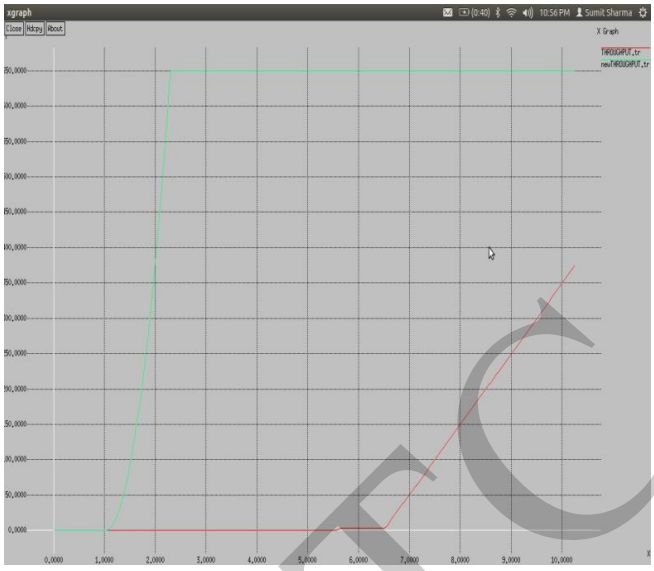

Fig4: Comparison graphs of Throughput

The throughput graphs of the previous and new techniques are shown in figure 4. The red line shows the throughput of previous technique and green line shows the network throughput of new technique.

V. CONCLUSION

In this paper, we conclude that many attacks are possible in wireless sensor networks. To prevent these types of attacks, sink movement technique has been proposed. The privacy is the main concern in the proposed technique. To ensure data privacy in the mobile sink cryptographically technique is been proposed in this paper.

REFERENCES

[1] Mariam Yusuf Hamdard Institute of Information Technology, Hamdard University Karachi, Pakistan "A Fuzzy Approach to Energy Optimized Routing for Wireless Sensor Networks" Vol. 6, No. 2, April 2009.

[2] Yimin Chen and Long Cheng Department of Electrical Engineering Stanford University "Query-Based Data Collection in Wireless Sensor Networks with Mobile Sinks" vol. 51, pp. 159–206,2008.

[3] Shahram Babaie, Javad Hasan-zadeh "New Active Caching Method to Guarantee Desired Communication Reliability in Wireless Sensor Networks" J. Basic. Appl. Sci. Res., 2(5)4880-4885, 2012.

[4] Narottam Chand, "Cooperative Data Caching in WSN" World Academy of Science, Engineering and Technology 63 2012.

[5] Md Ashiqur Rahman and Sajid Hussain, Jodrey School of Computer Science Acadia University "Effective Caching in Wireless Sensor Network".

[6] E. Ilker Oyman and Cem Ersoy Computer Engineering Department, Bogazici University, Istanbul, Turkey "Multiple Sink Network Design Problem in Large Scale Wireless Sensor Networks".

[7] D. Ganesan, B. Krishnamachari, A. Woo, D. Culler, D. Estrin, and S. Wicker, "An empirical study of epidemic algorithms in large scale multihop wireless networks,"

[8] Sooyeon Kim, Sang H. Son, Senior Member, IEEE, John A. Stankovic, Fellow, IEEE, and Yanghee Choi, Senior Member, IEEE "Data Dissemination over Wireless Sensor Networks"

[9] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, volume 5, Number 3, 2007, pp 338-346.