A New Approach to Enhancing Privacy and Performance in Opportunistic Wireless Sensor Network

Satpalsing D. Rajput[1] Dipak D. Bage[2] Sushant S. Bahekar[3]

Research Scholar *Research Scholar* *Research Scholar*

rajputsatpal@gmail.com *dipakdbage@gmail.com* *sushant.bahekar@gmail.com*

Abstract

Wireless sensor node senses the data from temperature, pressure and sound, and sends the packet through gateway. Those packets are routed or forwarded through a Gateway. Now a day's privacy is still challenging issue. In this paper the basic focus is on privacy of WSN and simultaneously performance of communication is also taken in consideration. The proposed architecture consists of central controller in which all registered node record should be stored. If any node wants to communicate with other node then it needs to broadcast all nodes with central controller. If identity of that Wireless Sensor Network not matched with central controller then node should be treated as blacklisted node and entire packet of that node should be dropped. Also performance will be enhanced after verifying that node.

Keywords: *Wireless Sensor Network, Registration Manager, Log Manager, Centralized Controller.*

1. Introduction

Wireless Sensor Networks are structured or unstructured dispersed nodes used to monitoring and recording the information in the ambient environment. WSN consist of hundred or thousand number of wireless sensor nodes that are dispersed each have its own battery embedded into the device, microcontroller and trans receiver which produced radio wave for communication purpose. Each node sensed the temperature, pressure and sound monitoring continuously by sensing these information through a gateway and forwarded to the base station. There are many attacks which causes the data sharing in between two consecutive nodes such as delay attacks, identity attacks, fishing attacks, warmwhole attack etc. WSN are classified into two types as Structured Wireless Sensor Network and Unstructured Wireless Sensor Network.

In Structured Wireless Sensor Network, the fixed numbers of nodes are articulated in one Ad-Hoc network. The number of nodes in the structured WSN is fixed and location of trusted node is diagnosed using GPS. But the structured nodes are internally fixed then there is no way to receive the GPS. So to choose the nearest GPS node must need to track the location of WSN. In trusted WSN the location, IP address and MAC address are important to prove the identity of node. It is necessary to protect a node in unsecure Ad-Hoc network and also important to forwarding and routing the data to authenticated node. These should be designed by proposed trusted location based opportunistic routing for security and authentication.

In Unstructured Location based Opportunistic routing the nodes are continuously move its location. So for identity purpose monitoring its location is not possible.

2. Literature Survey

In [1] authors presented privacy preserving APAC Protocol for access control. In which the authorized user are accountable to access the data, but there is problem with performance of communication. The proportion is such that if the privacy and accountability increases then performance of communication decreases.

In [2] authors presented the basic concepts of WSN, applications of these networks, design issues, and hardware constraints are involved. Also, they presented the protocol stack for sensor networks. The protocol stack discussed in this survey was a five layer network model. Authors raised a point that Ad-hoc routing mechanisms may not work well for sensor networks and more attention should be given for developing sensor oriented protocols. Energy constraint is the reason given by the authors for not using the traditional routing protocols for WSN. Authors have presented a discussion about the requirements of WSN like networking, security etc.

In [3] authors presented a detailed literature on routing protocols for wireless sensor networks and discussed various issues involved in these protocols. Authors have categorized the discussed routing protocols into three classifications i.e. location based, data centric and hierarchical routing protocols. The authors have discussed and presented each routing protocol in detail under each classification. Also, the methodology of each category was discussed and concluded with the open research questions. This is the issue related with how and when the data will be reported to the base station.

Paper [4] categorized the data reporting models depending on the types of applications. According to authors, the data reporting models may be based on event occurrence, query imposed by base station, continuous data delivery and hybrid. In event occurrence based data delivery model the nodes will communicate data to base station only if there is any activity occur in the area of deployment.

In [5] authors have proposed a trust and location aware routing (TLAR) protocol for WSN. The objective of TLAR was to provide a lightweight and dependable routing algorithm for WSN. TLAR consist of two main modules one is trust assessment and second is routing. Trust value was calculated on the basis of forwarding sincerity, packet integrity, network acknowledgements, energy, and secondary trust values. A consolidated trust value is calculated and the nodes which were having lower trust values, not included in routing process.

3. Proposed Methodology

In Below fig. 1 depicted Proposed Opportunistic Routing for WSN. Wireless sensor network in which different node forwarded or routed the information based on multi hop. Before forwarding the packets, each node allocated a session to transmit the packet to its consecutive next hop; here the next hop will be selected based upon confidence score of opportunistic network. When a session is initialize then each node querying with the central Controller node. This central controller has WSN Authenticator (WSNA) in which overall information of sensor node are registered in that registration manager. This information is in the form of MAC Address, IP Address, timestamp and physical location. Physical location depend upon the GPS location, if the geographic location for the node is external then GPS has no issue, but if it is internal node where GPS signal are not reachable then the distance of weaker signal GPS are measured. At initial level when session starts then each node will be verified base upon its identity if both node information and server details are matching then server delegate's ticket to requesting node. In this technique each node authorized by server and server broadcasts the ticket that is different for every other node. Now when packet forwarding starts then before that every node is present with its ticket. The node which has no ticket means in verification that node should be fail. So in this way the malicious node is encountered. Ticket has overall information that its identity is mentioned. If any malicious node tries to prove its fraud identity then it encountered in ticket authentication process. When the information is routed to consecutive next hop then its verified by public key which delegated by server to verified node.

Privacy is one of the challenging problem in wireless sensor network to establish such a framework which is reliable, energy efficient and privacy preserving by trusted third party. So the Proposed framework is established to resolve the problem. This Architecture consists of Query phase, Authentication phase, Communication phase and Termination phase.

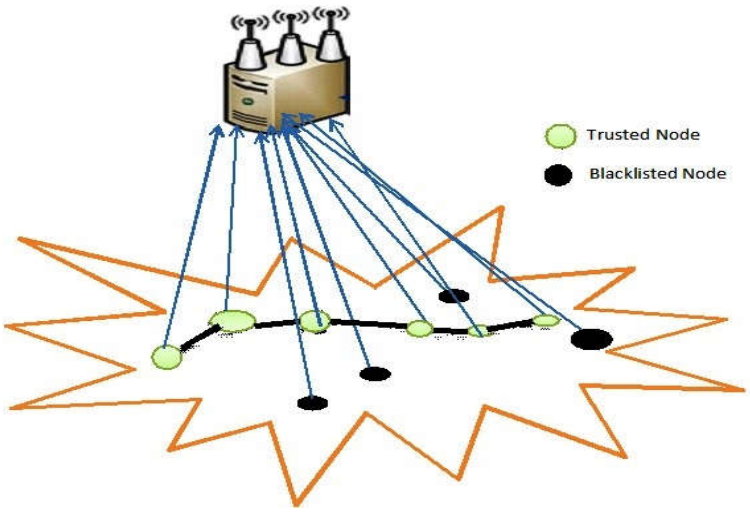

Fig 1. Proposed Opportunistic Routing for WSN

In opportunistic routing the sensor node forwarded or routed the traffic to such a node of which distance is less, and node efficiently reachable. But in such a case there will be problem of Sybil attack in which the malicious node is entered in the Ad-hoc network to update, delete or alter the data. So the confidence score is calculated to monitor such a node which is frequently routed data successfully. Therefore in opportunistic network if the two consecutive nodes are there on which one is such that whose distance is less but confidence score is zero in spite of that other have high confidence score but the probable distance is higher than first then such a case the second node is selected whose confidence score is higher.

$$Confidencescore(ConsecutiveNode) = \frac{\sum Confidencescore(Consecutivenode)}{\sum Confidencescore(Allnode)} \quad (4.1)$$

In above equation 4.1 Confidence score of Consecutive node is calculated which is Sum of Confidence Score of all Consecutive node to Confidence Score of all node. Wireless Sensor Network with opportunistic routing used the minimum distance to traverse from source to destination. The opportunistic routing is energy efficient technique by which a packet forwarded to the multi hop based on their distance between conjugative nodes.

Privacy Phases for Wireless Sensor Network

This Proposed methodology follows the following Phases.

A. Query Phase: Query phase is the primary process of proving identity. In which each node provide its identity to a Centralized Controller which is a centralized key distribution center and complete its verification by registration manager. The registration manager is one in which all the information related to wireless sensor node are registered at the time

of fixing the node. When the node querying to the registration manager then verification of node should be completed.

B. Authentication Phase: Once the node is verified then it is forwarded to the Log manager. Log manager is monitoring the log for the purpose of privacy. Each node delegated the log that log completely consist of node information as a payload file. Payload file is jar file were all the relevant data access information has been fed to the Payload file. The information is encrypted by using proposed WSN identity based encryption algorithm.

C. Communication Phase: Wireless Sensor Node is approved by controller then its permitted for communication. Then communication is established between the two consecutive nodes. Here the consecutive nodes are selected based upon the confidence score of that node. Now the first Wireless Sensor Node communicated with its consecutive next Wireless Sensor Node in secured channel having payload log file along with its sensor data. Means the data and payload file are encapsulated in one frame.

D. Acknowledgement Phase: Like that way the above three phases are repetitively executed for each node and apply the rule of confidence score based routing up to it reaches to the last node. Then it gives the acknowledgement to all nodes that previously visited.

E. Termination Phase: As the hop to hop communication is accomplished successfully up to the last node in stipulated time period that is mentioned in payload log file, then all the resources of node are terminated forcefully.

Proposed Algorithms:

I. Algorithm for Privacy in Confidence Score Based Opportunistic Routing.

The vital role of privacy preserving confidence score based opportunistic routing for Wireless Sensor Network algorithm is for enhancing energy efficiency by applying privacy constraint.

Step 1: Start
Step 2: Register all Wireless Sensor Node into the registration manager
Step 3: If node wants to send packet
Step 4: Then all node querying to Central Controller
Step 5: Central Controller verifying the details with log manager
Step 6: Log manager broadcast a ticket to all register sensor node that contain encrypted log file based upon the identity
Step 7: If (registration_manager_Details==Sensor_Node_Details)
Step 8: Then Node is Trusted
Step 9: Else
Step 10: Node is malicious Node
Step 11: Mark all malicious node as blacklisted node
Step 12: Dropped all packets permanently which is going to the Blacklisted node
Step 13: Perform hop to hop communications for each node
Step 14: Calculate Confidence score of opportunistic routing
Step 15: Repeat Step 1 to Step 14 for all Trusted Nodes
Step 16: Encapsulate frame with Encryped payload log file to Next hop
Step 17: If (EC First_Hop==EC Next_Hop)
Step 18: Established Secure channel for Communication
Step 19: Send acknowledgement from Destination node to Source node
Step 20: Finally terminate all resources forcefully.
Step 21: Stop.

II. Algorithm for Identity Based Encryption

This algorithm perform encryption based upon Identity of user. For this it require the different parameter such as MAC address, IP address and GPS Location [6].

Step 1: Start
Step 2: GenKey (MACAddress, IP Address, GPS Location) Registration manager verify and create encrypted Payload file.
Step 3: Encrypt(ENC): Registration Manager Encrypt key and send public key WSN Node.
Step 4: Decrypt (ENC):WSN Node Decrypt key based upon public key.
Step 5: Stop.

4. Conclusion

Proposed Confidence score based Opportunistic routing algorithm should be removed malicious nodes from the network. Only trusted nodes that are registered in central controller of Wireless Sensor Node are able to transmit the packet. So that the privacy should be enhanced as well it diagnosed the parallel path which has less cost and resources. By applying this technique the privacy and performance of WSN will be improve.

References

[1] Daojing He, Sammy Chan and Mohsen Guizani "Accountable and Privacy-Enhanced Access Control in Wireless Sensor Networks," IEEE Transactions On Wireless Communication., vol.14, No.1, (2015) pp. 389-398.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," Computer networks., vol. 38, no. 4, (2002), pp. 393-422

[3] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," Ad hoc networks, vol. 3, no. 3, (2005), pp. 325-349,.

[4] K. Sohrabi, J. Gao, V. Ailawadhi and G. J. Pottie, "Protocols for self-organization of a wireless sensor network," IEEE Transaction on Personal Communications, vol. 7, no. 5, pp. 16-27, 2000.

[5] P. R. Vamsi and K. Kant, "Trust and Location-Aware Routing Protocol for Wireless Sensor Networks," IETE Journal of Research, vol. 63, (2016), pp. 1-11.

[6] Bhole, Ashish T., and Satpalsing D. Rajput. "Ensuring Accountability for Application Sharing in the Cloud." In Proceedings of IEEE International Conference on Computational Intelligence and Computing Research (ICCIC),Madurai, India, (2013), pp.148-152,26 -28.