International Journal of Academic Research and Development
ISSN: 2455-4197, Impact Factor: RJIF 5.22
www.academicsjournal.com
Volume 1; Issue 1; Jan 2016; Page No. 79-82

A study on communication issues and methods in sensor network

Parveen
M. Tech (Department of Computer Science & Application) CDLU, Sirsa, Haryana, India.

Abstract
Sensor network characterization lies relative to the environment and application in which it is applied. The network suffers from various communication and architectural challenges. These challenges results various network attacks and communication deficienes. In this paper, a study on sensor network characterization and associated issues is provided. The paper also identified various communication methods to provide the safe and reliable communication in the network. A study on the work provided by earlier researchers on communication methods is also provided in this paper.

Keywords: WSN, Communication Challenges, Communication Methods

Introduction

Sensor Network is a bunch of sensor devices connected in real environment to capture the sensitive information. In WSN these sensor devices are known as wireless sensors, which simultaneously adds to the network and forward the data. Figure 1 shows about WSN, transmission in wireless sensors can be done by making air as a medium, as per the figure wireless node can be bodily attached to a motor vehicle, or to a jet to make wireless communication among them.

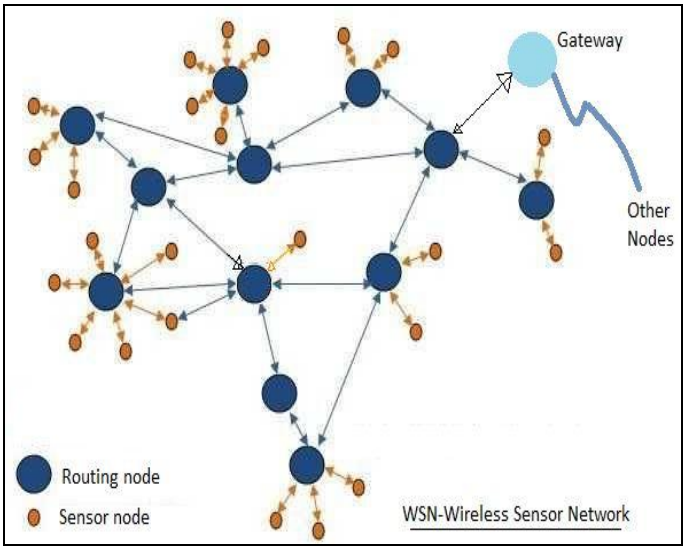

Fig 1: WSN Transmission

In WSN for transmission, a wireless node may be the source, the goal, or an intermediate node. When the wireless sensors are acting as an intermediate node then it performs as a router. Such router can accept and transmit the information packets to its adjacent neighbor. In the wireless atmosphere, all sensors keep on moving rather than being stagnant. Therefore, the wireless topology does not remain same all the time. WSN environment has some limitations for example this network is a self-organizing network. The biggest issue of such network is that the topologies keep on changing because of the movement of the sensors in the wireless network. In such type of network all sensors act as participants and as well as routers. Due to the wireless communication and continuous change in topology there is a large probability of different types of misbehaviors and loss in the information packets.

Security is very important concern because of the weakness like Dynamic topology, wireless links, Cooperativeness or Limited resources, packet loss due to error in transmission and route changes due to mobility and many other challenges. Network security is very important and difficult task because no single security solution is enough for the network. WSNs Characteristics, features, advantages and different types of communication characterization are defining below:

Network Characteristics

Ad hoc Networks are example of networks which offers unlimited mobility without any basic infrastructure. Basically, WSN is a set of sensors that passes data to each other by making a multi-hop network. Characteristics of WSN are shown below:

1. Dynamic Topologies: Sensors are free to move in the wireless network. Sensors move in a random manner and because of this random movement the topology of the network also changes in an unsystematic manner. As a result directional and unidirectional links are formed between the sensors.
2. Energy Constrained Operation: Sensors in the wireless system depends on the energy source like batteries. Numbers of tasks are performed by the sensors when they consume more energy. So, energy should be properly utilized in the network.
3. Bandwidth Constraint: If we compare the efficiency of wireless network to the wired network than wireless has less capacity. Wireless network is less efficient because of several reasons like fading, noise and interference etc. Due to all these reasons clogging (congestion) occurs in the network and it is a big problem in bandwidth utilization.

4. Limited Physical Security: WSN are usually more open to physical security threats compared to wired networks because the WSN is a scattered system and due to this, chances of eavesdropping, spoofing, masquerading [1,2] increases.

Communication Features

1. Autonomous Terminal: In Ad hoc Network, every sensor terminal is an independent node. This node can act in many ways, it can act as a host and it can act as a router. Sensors can also behave as switching functions like a router. So, the end point and the switches cannot be identified independently.
2. Distributed Operation: Circulation of control and management is done between the terminals in order to have vital control over the network operations. In order to execute a function like security or Communication, the sensors must pair with themselves and independent node must behave as a relay.
3. Multi-hop Communication: Ad hoc Communication algorithms can be differentiated on the basis of Communication protocol and link layer attributes. They can be classified as single hop algorithm and multi hop algorithm. Multi hop algorithm is more complex as compared to single hop because of its structure. During transmission of information, the packets should cross more than one intermediate node.

Related Work

A sensor network is critical network suffers from various data level communication irregulateries. To provide the safe data communication various author provided different methods at different layers and protocols. These methods are either against some misbehavior or based on communication deficiencies. Author [1] proposed a method called Communication algorithm that mitigates blockage misbehavior by analyzing destination sequence number and validating the destination by random value. In this technique, Simulation output show that the increasing packet delivery ratio when compared to protocol in presence of blockage misbehaviors. Author [2] proposed a solution to identifying and preventing the cooperative misbehavior between nodes. The proposed technique, identifying and remove the cooperative sensors from the network and provide secure path from source to destination node. Author evaluates the proposed solution and compares it with other existing solutions in terms of throughput, packet loss percentage, average end-to-end delay and route request overhead. Author [3] an approach is proposed to combat the safety by using negotiation with neighbors who claim to have a route to destination. The Simulation's results show that the proposed protocol provides better security and also better result when packet delivery performed. And this technique is better than the conventional MAC protocol. This is used for the blockage with minimal additional delay and Overhead.

Author [4] a review on a major category of coordinated deficienes in the network A which are a serious threat to ad hoc network security. In cooperative misbheioaur can be identified multiple sensors collide to hide the malicious activity of other sensors; hence such misbehaviors are more difficult to detect. Author [5] Author addressed the problem of coordinated misbehavior by multiple blockages acting in group. Author presents a technique to identify multiple blockages cooperating with each other and a solution to discover a safe route avoiding cooperative blockage misbehavior. Sensor Network is a collection of sensor node. In WSN, all sensors commonly move randomly and dynamically because it is a temporary network without a network infrastructure. A malicious node send Route Response (RREP) incorrectly of having route to destination with minimum hop count and when sender node transmit the data to the malicious node, then malicious node drops all the packet in the network [6]. Author [7] presents RBS (Reference Broadcast Synchronization) & Relative velocity distance method is used for detect the cooperative node by using the clock synchronization process in WSN. This evaluates the performance in NS2 network simulator and presented analysis indicates that this method is very suitable to remove blockage misbehavior. Author [8] proposed an opinion based cooperative trust model to improve the performance of network, particularly in the presence of malicious sensors. In this model, each node with respect observes the behavior of other sensors and then determines the trustworthiness of the other sensors. In this model two trusts are given direct and indirect, first is when it gain the direct trust by the information obtained independently of other sensors or second one is when indirect trust information obtained via opinion of other sensors.

Author [9] proposed a novel method to enhance security in both phases. Author present the design of a Communication protocol based on trust, which ensures secure and undisrupted delivery of transmitted data. In this method, for self-encrypt the data without the necessity of a cryptographic key, an end to end encryption technique is used. Author have many are characteristics like wireless sensor connectivity, randomly changing topology, distributed operation and ease of deployment. The work proposed work is used to detect the blockage misbehavior using Modified Associatively Based Communication protocol (MABR) which is the modification and improvement of Author [10]. Author [11] proposed a novel opinion based trust-aware Communication protocol (OBTRP) for WSNs to protect forwarded packets from intermediary malicious sensors. In this model, each node with respect observes the behavior of other sensors and then determines the trustworthiness of the other sensors. In this model two trusts are given direct and indirect, first is when it gain the direct trust by the information obtained independently of other sensors or second one is when indirect trust information obtained via opinion of other sensors. Author [12] proposed a comparative analysis of Blockage misbehavior for both Proactive and Reactive protocol. The impact of Blockage misbehavior on the performance of VCN as well as Sensor Network is evaluated and then find out which protocol has more vulnerable to the sensor misbehavior and how much is the impact of the

misbehavior on both protocols. Author [13] performed the survey on Cooperative Misbehavior in WSN. WSN is a bunch of wireless sensors. WSN sensors are due to the wireless links these sensors are connected automatically as per defined the Communication protocol in the network. In this author has defined the problem of packet forwarding by the misbehavior sensors and also proposed a mechanism for blockage misbehavior and greyhole misbehavior and remove them.

Wsn Communication Challenges

Such kind of network is explained [147] under the feature guidance at node as well as network level. The network is explained with variable position as well as fixed position scenarios. The location of sensors is explained under mobility guidance and narrow range setting under the implication of stability. The network is explained under the limitation of route identification and volume limit guidance. The network is explained under the node neighbor identification that can identify the efficient next hop to create the effective communication route over the network system. The hop recognition can be finished with the range and other parameters guidance. The Communication approaches adapted by different Sensor Network are shown and discussed. These approaches are given below figure 2.

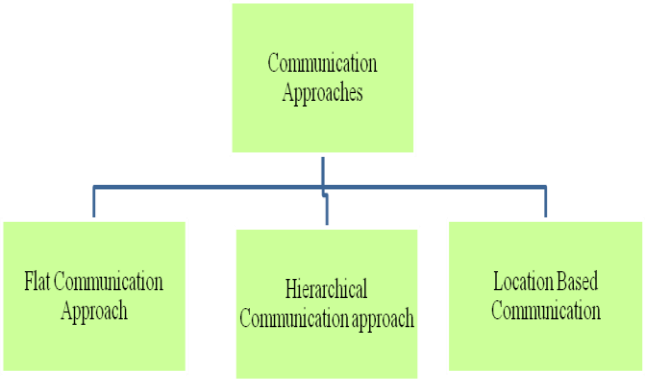

Fig 2: Communication Approaches

A) Flat Based Communication

Such kind of Communication technique is used in identical network with randomized parameters guidance. All the network sensors are of same type and the multi hop route is used to optimize the network route. In most of the intra- cluster Sensor Network, these kind of Communication approach is been used to carry out the network communication. This Communication approach works on the destination adaptive and data adaptive communication carried out over the network. The network also has the multi case communication to minimize the communication effort. To carry out the multi cast communication aggregative communication approach is adaptive in these networks. Such kind of Communication technique also requires minimizing the number of intermediate sensors as well as minimizing the communication effort of each involving node over the network. Such kind of communication route read the next neighbor under different physical and communication parameters and choose the node with effective throughput and minimum expected loss and delay. The work is about to minimize the flooding by capturing the Communication information as well as minimize the redundancy in communication. The work is also effective to carry out the broadcasting of the network as well as effective hop selection over the network.

B) Hierarchical Communication

In this Communication technique, the inter cluster communication is carried out. The sensors can identical or different but the sensors in a same network are considered as identical. The network area chosen in this network type is generally big and measurable. Each sub network is explained under the guidance of controller node so that the effective network aggregation will be carried out by the node. This controller node takes the adaptive decision regarding the node guidance and the sub network head specification. The segmented communication is made in the form of tree and at each tree node decision regarding the adjacent network election will be done.

C) Location Based Communication

The Communication technique explained here for the guidance of network node and tracking of node under the location guidance and creation. This Communication technique relies on the node location and the signal strength of various positions over the network. The satellite guidance is used to select the position of the node and to carry out the activity of the network under guidance of protocol. GPS analysis is carried for node location monitoring and indication to select the node and to perform the zoning of the network with guidance of the criticality for the network with specification of Communication and mobility.

Conclusion

In this paper, a rule adaptive trust evaluation model is provided to generate the safe communication in sensor network. At first level of this model, the node level evaluation is applied on stability, coverage and direction parameters. Based on this analysis, the zones are generated over the network path. In second stage, the each zone is analyzed under packet loss, response time and delay parameters. Based on these parameters, the trust weights are assigned. Finally, 27 rules are applied to generate the effective route over the network. The simulation results shows that the method has reduced the communication delay and communication loss.

References

1. Rajesh Yerneni. Enhancing performance of AODV against Blackhole Attack, CUBE Pune, Maharashtra, India, ACM, 2012, 978-1-4503-1185-4/12/09.
2. Hesiri Weerasinghe. Preventing Cooperative Blackhole Attacks in Mobile Ad hoc Networks: Simulation Implementation and Evaluation", International Journal of Software Engineering and Its Applications, 2008; 2(3).
3. Mehdi Medadian. Detection and Removal of Cooperative and Multiple Blackhole Attack in Mobile Ad hoc Networks, International Conference

on Computer and Software Modeling, IPCSIT, IACSIT Press, Singapore, 2011, 14.
4. Sweta Jain. A Review Paper on Cooperative Black hole and Gray hole Attacks in Mobile Ad hoc Networks, International Journal of Ad hoc, Sensor & Ubiquitous Computing, (IJASUC), 2011; 2(3).
5. Sanjay Ramaswamy. Prevention of Cooperative blackhole Attack in Wireless Ad hoc Networks, 2011.
6. Varsha Patidar. Black hole Attack and its Counter Measures in AODV Routing Protocol, International Journal of Computational Engineering Research, (ijceronline.com), 2(5).
7. Harsh Pratap Singh. Guard against cooperative black hole attack in Mobile Ad hoc Network, International Journal of Engineering Science and Technology (IJEST), ISSN: 0975-5462, 2011; 3(7):
8. Poonam. Eliminating misbehaving sensors by Opinion based Trust Evaluation Model in WSN's, ICCCS'2011, Rourkela, Odisha, India, ACM 978-1-4503-0464-1/11/02.
9. Poonam Gera. Trust Based Multi-Path Routing for End to End Secure Data Delivery in WSN's, SIN'2010, Taganrog, Rostov-on-Don, Russian Federation, ACM 978-1-4503-0234-0/10/09.
10. Shobana M. Geographic Routing used in WSN for Black hole Detection, CCSEIT-2012, Coimbatore, Tamilnadu, India, ACM 978-1-4503-1310-0/12/10.
11. Poonam. Misbehaving sensors Detection through Opinion based Trust Evaluation Model in WSNs, International Conference and Workshop on Emerging Trends in Technology (ICWET 2011), TCET, Mumbai, India. ACM 978-1-4503-0449-8/11/02.
12. Kamaljit Kaur. Comparative Analysis of Black hole attack over Cloud Network using AODV and DSDV, CCSEIT'2012, Coimbatore, Tamil nadu, India, ACM. 978-1-4503-1310-0/12/10.
13. Revathi B. A Survey of Cooperative Black and Gray hole attack in WSN, International Journal of Computer Science and Management Research, 2012; 1(2). ISSN: 2278-733X.