Selective Forwording Attack Detection Using Channel Quality Reputation Analyzer In Wireless Sensor Networks

[1]M.Ramkumar [2]K.Aravindkumar
[#1] Research Scholar, [#2] Assistant Professor
[#1]Department of Computer Science and Engineering, MS University Tirunelveli.

Abstract - The Wireless Sensor Network is an accumulation of sensor hubs gathered together for accumulation of extensive variety of mission basic information, for example, acoustic signs, weight, temperature, application. Security is the genuine subject in remote sensor systems. Along these lines, WSNs are powerless against different sorts of security assaults. Particular sending assault is an uncommon instance of dark gap assault where traded off hubs drop parcels specifically. This prompts corruption of system execution. The proposed framework changed the recognition framework utilizing Channel and Quality Reputation Analyzer (CQRA) that can productively distinguish the particular sending mischief from the ordinary misfortunes. The proposed strategy two distinct systems, Channel Reputation Identification (CRI) and Data Traffic Reputation Identification (DTRI). If information misfortune rate at specific hubs surpasses over the assessed typical misfortune rate, those hubs utilized for correspondence will be set apart as aggressors. The principle preferred standpoint of the proposed strategy is, brought together notoriety table in judge hub with the goal that lessens correspondence and directing overhead. The bundle conveyance proportion will be expanded when contrasted with other existing techniques. Additionally, CQRA accomplish a high location precision with both of false and missed identification probabilities and enhance over 20% bundle conveyance proportion for the system. The proposed examination recreated utilizing system test system NS2. The counteractive action procedure is essentially fruitful in taking care of the assault, while reestablishing the execution of system and decreases the impact of assault from the system.

Keywords - Selective forwarding Attack, CRS-A, CQRA, WSN

1. *INTRODUCTION*

WSN alludes to a collection of spatially disseminated and dedicated sensors for observing and recording the physical states of the earth and arranging the gathered information at a focal area. WSNs measure ecological conditions like temperature, sound, contamination levels, dampness, wind, etc., Sensor hubs have capacity to gather detected information and send that to the base station, a WSN for the most part comprise of a base station that can speak with various remote sensors by means of radio connection. WSN utilizes a remote channel to convey, so there are definitely a few issues, for example, message capture, altering and other security. Along these lines, the security of systems importantly affects the execution of observing, framework access. In a selective forwarding attack, malicious nodes may refuse to forward certain messages.

2. *SELECTIVE FORWARDING ATTACK*

In a specific sending assault, pernicious hubs may decline to forward specific messages and just drop them, guaranteeing that they are not proliferated any further. A foe inspired by stifling or altering bundles starting from a chosen few hubs can dependably forward the rest of the activity and point of confinement doubt of her bad behavior. The particular sending assaults can be of various kinds. In one sort of the specific sending assault, the vindictive hub can specifically drops the parcels originating from a specific hub or a gathering of hubs. This conduct causes a DoS assault for that specific hub or a gathering of hub. Another sort of particular sending assault is called Neglect and Greed. In this shape, the subverted hub subjectively fail to course a few messages

3. *EXISTING SYSTEM*

In the current System, a Channel-Aware Reputation System with Adaptive Detection Threshold (CRS-A) to identify specific sending assaults in Wireless Sensor Network. To recognize particular sending assaults from the typical bundle misfortune got from the ideal assessment limit of CRS-An in the probabilistic way, which is versatile to the time-shifted channel condition and assault probabilities of traded off hubs. In CRS-An, every sensor hub keeps up a notoriety table to assess the long haul sending practices of its neighboring hubs. Once the notoriety estimation of a senor hub is underneath a caution esteem, it would be distinguished as an ordinary hub. As opposed to segregating all the traded off hubs from information sending, it mutually considers the time-differed channel condition and assault probabilities of neighboring hubs in picking sending hubs. Location of particular sending assaults turns out to be additionally testing, if the typical bundle misfortune rate is more fluctuant and hard to appraise because of the versatility of sensor hubs designations.

DISADVANTAGES OF EXISTING SYSTEM

- Cannot identify the exactly node is misbehaving node using reputation table
- Data access delay is more
- Data access delay is more

4. PROPOSED SYSTEM

Channel and Quality Reputation Analyser (CQRA) strategy can recognize the specific sending assailants by sifting through the typical channel misfortunes. The Channel Identification is coordinated with Data Traffic Reputation Identification (DTRI) to accomplish channel-mindful recognition of particular sending trouble making covered up in the ordinary misfortune occasions because of awful channel quality or medium access crashes. Estimation of parcel misfortune because of remote channel quality, named as remote misfortune likelihood, by demonstrating the fundamental time fluctuating remote channel. In CQRA, assault location depends on the blend of downstream and upstream observing. The downstream/upstream checking suppositions are arranged by contrasting the observed misfortune rates and the downstream/upstream discovery limits. Because of the irregularity nature, even without particular sending assault, a burst of typical misfortune occasions in specific circumstances may prompt the false alert. A false clear or missed discovery happens when the identification plot does not give an alert but rather a risk exists. Likewise inferred that both upstream and downstream checking is fundamental for precisely identifying the aggressors.

ADVANDAGE OF PROPOSED SYSTEM

- Can detect the attackers efficiently and increased the packet delivery ratio of the network
- Minimize the false alarm and missed detection probabilities
- PDR is improved

5. CHANNEL QUALITY REPUTATIVE ANALYZER

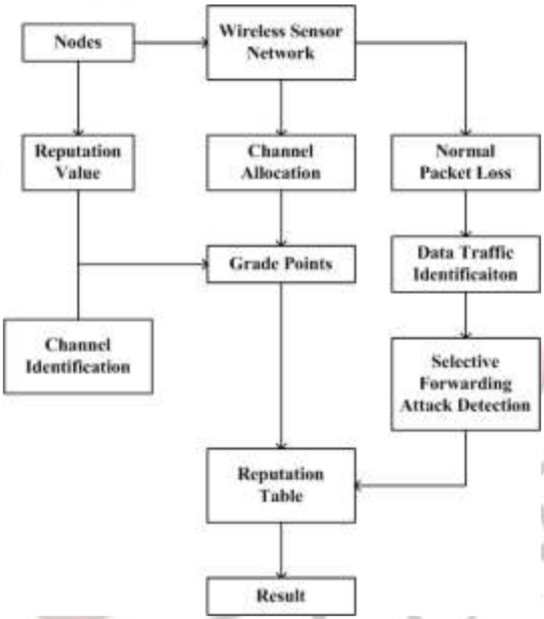

Fig 5.1 Block Diagram

1. *DATA REPUTATION IDENTIFICATION*

Notoriety Analyzer has as of late been proposed as a viable security instrument for open and dispersed condition. Basically, the hubs that don't act appropriately will have low notoriety, so whatever is left of the hubs will keep away from any cooperation with them, which is identical to its detachment from the system. There are various meanings of trust and notoriety, yet basically trust is a conviction about future conduct that one hub holds in others and it depends without anyone else encounter, hence its principle trademark is subjectivity. Then again, notoriety is thought to be the worldwide impression of the conduct of a hub in light of the assume that others hold in it, in this manner thought to be objective. Other options to notoriety frameworks can be motivation frameworks, where it is worthwhile for the hubs to act in a way that the subsequent worldwide welfare is ideal.

DTRI approach offers many advantages. Since it does not use reputation information from other nodes, it is resilient to badmouthing attack which is one of the main vulnerabilities of standard reputation systems. Furthermore, it confines attacked nodes faster while relying on much lower node redundancy than standard reputation systems

In order to provide uninterrupted network operation, core network protocols (aggregation, routing and time synchronization) have to be secured. Regarding the attacks on the aggregation protocol, we assume that they demonstrate themselves in skewed aggregated values, which can be the result of either a number of skewed sensed values, or a compromised aggregated node. The proposed algorithm has been tested on a simulator of sensor networks developed by our research group and designed using the C++ programming language. Behavior Analysis uses overlapping populations, where the worst 40% of individuals are exchanged in each generation. In the following experiments NB has 20 individuals, evolved during 50 generations, with respective crossover and mutation probabilities 0.6 and 0.05. Selection is performed using standard roulette wheel approach. The computational time of GA under these settings is measured in minutes. Furthermore, it has been demonstrated that the presence of detection algorithms increases the efforts the attacker has to introduce in order to compromise the network.

2. *CHANNEL REPUTATION IDENTIFICATION*

A portable host imparts to the system through a radio access purpose of its correspondence run. While it leaves scope of one access point, it interfaces with the new access point inside its range and begins conveying through it. The second approach is to frame a specially appointed system among clients needing to speak with each other. This implies every single portable hub of these systems carry on as switches and participate in recognition and upkeep of courses to other versatile hubs in the system. This kind of systems administration is constrained in run by the individual versatile hub transmission range and it is commonly littler when contrasted with the scope of cell frameworks.

In this way it is utilized to build the system lifetime and calculations recognize the accessibility channel for the gadget and routinely check the impedance and malignant hub in the gathering of the hubs of the group. On the off chance that any obstruction recognized it should substitute the channel or if any pernicious hub is experienced it disregards the way shaped along the specific hub.

Then the mobility of each node is compared and the node with least mobility is selected as cluster head. If not then the nodes is labelled as ordinary node. Alive messages are sent to all the nodes and the response time is calculated for each node and the node with highest response time is selected as the next cluster head. Important factor in deciding the cluster heads. In order to avoid frequent cluster head changes it is desirable to elect a cluster head that does not move very quickly. When the cluster head moves fast, the nodes may be detached from the cluster head and as a reconfiguration occur.

According to the network model, normal packet loss is mainly caused by the poor and unstable wireless channel and MAC layer collisions. The poor and unstable radio link quality is the primary reason for the time-varied packet losses. It is formulated as a two-state Markov model, and the packet loss rate is determined as an average value over a long-term period. However, adopting an average value to represent a time- varied value may mislead the evaluation for forwarding behaviors. Furthermore, dynamic environments make the link quality varied in different locations. In CRI, the link quality estimation for each pair of neighboring nodes is based on the Received Signal Strength Indicator (RSSI) and Signal-to-Noise Ratio (SNR), under the symmetric channel assumption. As data transmission between two neighboring nodes is based on the IEEE 802.11, MAC layer collisions may increase the normal packet loss rate. Since sensor nodes are static in our network, it means each sensor node has a fixed number of neighboring nodes. Then, we can use the analytical results in to estimate the packet loss caused by medium access collisions without the impact of hidden terminals.

6. PERFORMANCE EVALUATION

The recreation comes about are gotten under a few trials .The outcomes for proposed work has been contrasted and the aftereffects of CQRA convention utilizing X-graph. XGRAPH has been utilized to direct subjective examination. The parameters thought are Packet conveyance proportion, Average Delay or End-to-End Delay, Throughput, Packet Loss and Energy. The accompanying graphical investigation demonstrates the execution aftereffects of CRS-A and CQRA techniques

A. MEMORY CONSUMPTION FOR ROUTING

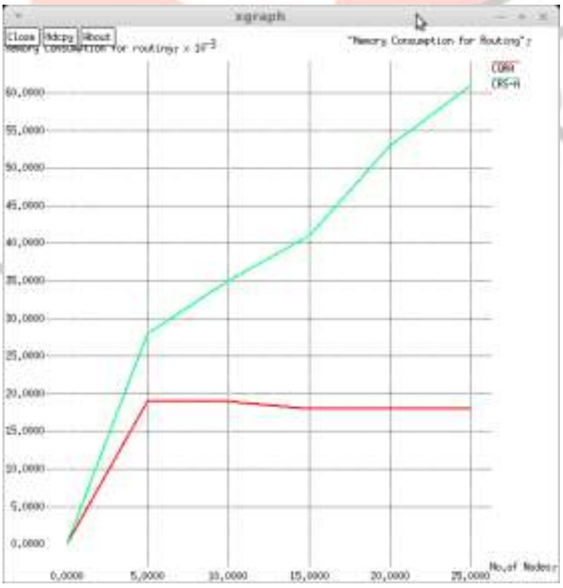

Fig. 6.1 Memory Consumption for Routing

The xgraph for CQRA and CRS-A x-axis indicates no of nodes in the graph and y axis indicate the memory consumption for routing to represent the graph. The graph shows 60.00 for CRS-A and 20.00 for CQRA.

B. PACKET DELIVERY RATIO

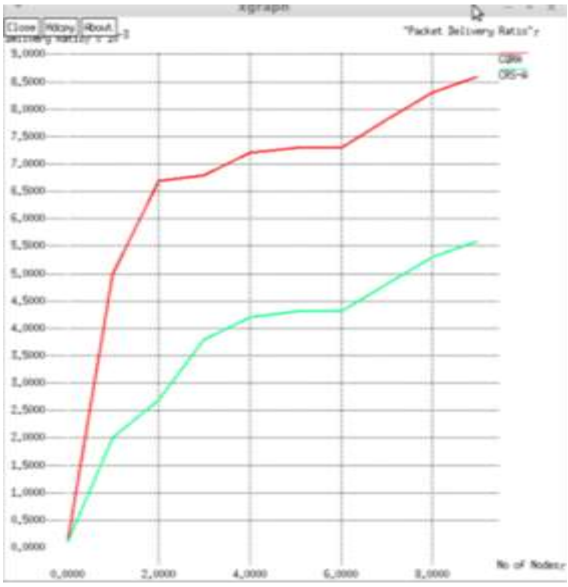

Fig. 6.2 Packet Delivery Ratio

The packet delivery ratio (PDR) is based on the number of packets received and generated in the trace PDR file is defined as the ratio between the received packets by the destination and generated packet by the source packet delivery is calculated using script which process. The trace file produces the result.

C.AVERAGE END TO END DELAY

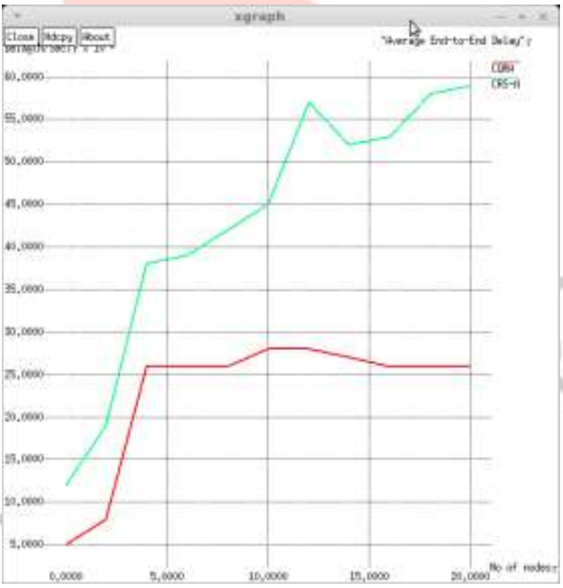

Fig. 6.3 Average End to End Delay

Delay in the difference between time and which sender is generated the packet and which receiver receive the packet delay is calculated using awk script which processes the trace file which produces the result. In this graph x axis indicates the no of nodes and y axis indicates the end to end delay in the packet ratio

D.HOP COUNT

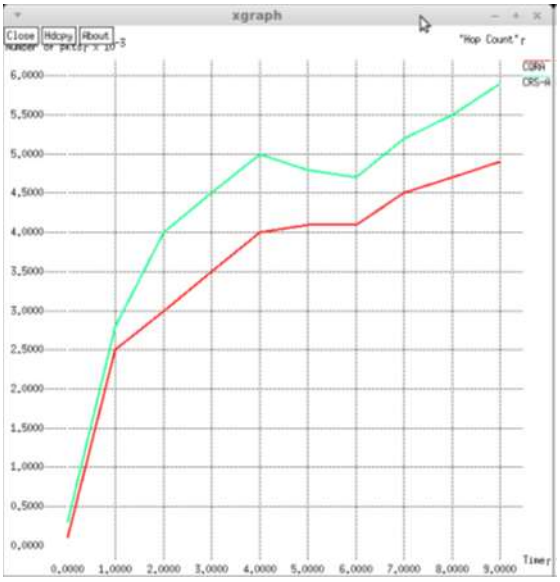

Fig. 6.4 Average Hop Count

Wireless communications are used to special purpose and thus the maintenance of energy efficient routing is the one of the largest problem and the most challenging in recent days routing path selection based on packet delivery ratio and hop count energy requirement is already proportional to the hop count and inversely proportional to the packet delivery .so the reliable protocol using uses degree of path selection which is based on hop count and packet delivery for the path selection. The graph x axis indicates number of nodes and y axis indicates Hop count.

7. *CONCLUSION*

A project, propose a simple and efficient security scheme for detecting selective forwarding attacks. The attacks which affect it as in malicious node attack drop the packet and make it unavailable to destination. This type of attacks is important to meet the basic need of the n/w. So a Channel Quality Reputation Analyzer (CQRA) method is developed that can efficiently identify the selective forwarding attackers by filtering out the normal channel losses. The Channel Reputation Identification (CRI) is integrated with Data Traffic Reputation Identification (DTRI) to achieve channel-aware detection of selective forwarding misbehavior hidden in the normal loss events due to bad channel quality or MAC. These utilize the metric ETX to defend against selective forwarding attacks. Then proposed a Centralized Algorithm that assigns a central node to collect and analyze the forwarding behaviors of each node in the network. The simulations have shown that the proposed algorithms can detect the malicious nodes participating in selective forwarding attack with high successful rate and it is efficient in terms of computation and communication overhead. Currently this scheme can only discriminate abnormal packet loss from channel error packet loss at a high detection ratio

8. *FUTURE SCOPE*

The proposed review all existing technique and developed a better technique to detect selective forwarding attack; future scope of this study is to provide the researchers all the drawbacks of existing schemes so that they can develop better and efficient detecting scheme. For future work, modelling more Do's attacks on the routing layer, including spoofing attacks that manipulate packet content and are significantly more difficult to detect selective forwarding attack. The future analysis is to employ different classification techniques, such as neural networks and k-means nearest neighbors and gauge how these systems perform in this application in comparison to Naive Bayes. Also, it would be interesting to make our intrusion detection scheme distributed and measure whether the detection accuracy of low participation selective forwarding attacks becomes more efficient. If so, would like to measure the trade-off between detection accuracy and energy depletion in the network.

9. *REFERENCES*

[1] Bo Yu and Bin Xiao, "Detecting selective forwarding attacks in wireless sensor networks," Parallel and Distributed Processing Symposium, 2006, 20th International, page 8 pp., 2006

[2]I Chris Karloff and David Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," Ado Networks (Elsevier), Sept, 2003.

[3] Jiang changing and Zhang jamming, "The selective forwarding attacks detection in WSNs", Computer Engineering, 2009, 35 (21):140-143.

[4] P Wang Xing-sheng, Zhan Yong-Zhao, Xing Shaming, Wang Liang in, "Lightweight Defence Scheme against Selective Forwarding Attacks in Wireless Sensor Networks' pp.226-232, IEEE, 2009.