Mitigation of Sink Hole Attack with QoS based Multipath routing in Wireless Sensor Networks

Dr. V.Sireesha[1] K Santosh Kumar[2]

[1]Assistant Professor, Dept.of CSE, Vasavi College of Engineering, Ibrahimbagh, Hyderabad, Telangana, India

[2]M.Tech Student, Dept.of CSE, Vasavi College of Engineering, Ibrahimbagh, Hyderabad, Telangana, India

Abstract

Wireless Sensor Networks (WSNs) were mainly composed of sensors with self-regulation capability that track physical or environmental conditions such as pressure, temperature, movement, sound, and so on. The main threat to the WSN network layer is sinkhole attack and this was still a difficult problem for sensor network to detect packets from other usual sensor nodes. In order to detect intrusions in the Network using LEACH (Low Energy Adaptive Clustering Hierarchy) protocol, the present paper proposes an intrusion detection system (IDS) to mitigate Sink Hole Attack. In proposed algorithm for measuring the intrusion (IR) ratio the detection methodologies, including the amount of packets transmitted and received, were utilized by IDS department. It can then overcome the weak attack of sinkhole. The results of the simulation are seen above all in terms of minimal delay, an improved delivery ratio, higher network efficiency and low energy utilization in proposed algorithm compared to current research QoS-MRP. Algorithm was also analyzed numerically with Ns-2.

Keywords: Energy Efficiency, Intruder Attacks, Intrusion Detection System, QoS, WSN, Multipath Routing, Sink Hole attack.

I. Introduction

A large node of small wireless sensor nodes is a WSN network. There are small batteries, limited power and a limited microprocessor at the sensor nodes. These sensor nodes primarily aim to collect and transfer the collected information from all neighboring nodes to base station (BS) or sink [1]. WSN applications [2], [3] are diversified in a range of ways including civil, military, and disaster-management systems, video tracking, intrusion detection and imagery.

The protection of a system or network was affected mainly by an intrusion. Intrusion was an operation that may influence QoS of Network through its effect on its integrity and energy

efficiency. Intruders are identified and tracked by IDS, a security system. The network is secured by the IDS system. The first step of an IDS is the identification of the route or link followed by a malicious attack. An IDS is becoming rather repetitive when the primary target of the network is the high value detection rate for attacks (DR) along with the low FAQ [4]. In a large number of details, in the modern era of real time devices, the identification of an intruder is a difficult task. The best approach for finding trends from two main process data is data mining: data classification and data selection. Data collection is the best solution. It is one way to track intruder without affecting WSN's QoS. Intrusion detection was seen as an object tracking process that tracks a wide range of malicious attacks using an energy conservation mechanism to increase system lifetime.

Multi-path routing may be considered an appropriate WSN fault and intrusion tolerance routing protocol, and therefore data communication and delivery. This protocol primarily aims to boost WSN's IDS by expanding its service life [5]. The protocol also provides reliability for QoS, maximizes WSN life and minimizes the delay that meets all QoS requirements. The high demands for QoS are significantly considered for most QoS criteria, like delay jitter, bandwidth and packet lower ratio. Thus, multi-path routing algorithms and even the detection of intruders if a sinkhole attack occurs meet WSN specifications for real-time application with high speed. The multi-path algorithm minimizes the resources used in multi-path communication. The number of costs of multipath tree links should be reduced to achieve this goal. We will talk about the shortest algorithm of Dijikstra's path.

This paper focuses on the IDS, which identifies malicious nodes, as a high-level security mechanism. The malicious node begins the attack by stating that the BS node is nearest and absorbs packets and changes transients. If a node can manage the network and control the packets, it remains a weakness in the event of insider attacks. Most protocols for network routing sensors do not trigger the detection of security attacks. Encryption and authentication mechanisms are typically inadequate for laptop and intrusion attacks. Thus, a defense against such attacks has become imperative. Major goal of this work of research was to study and design a security feature that will help overcome the adversity of sinkhole attacks in WSN that utilizes the LEACH protocol for its routing operations. Insiders or external attackers on a WSN cause sinkholes. A strong detection sinkhole attack is detected by the proposed IDS algorithm.

II. Literature Survey

In [6, 7, 8, 9 and 10], many protocols for QoS routing were proposed for wireless network based on network dynamics. While these protocols considered the QoS criteria, they considered energy conscience rather than unreliable state details to define routes. These protocols considered the best routing effort results and average response time was traditionally been regarded as key concern for QoS. Within [11, 12], author QoS routing is proposed, but the WSN does not have limited resources, restricted with real time Multimedia data.

The QoS-based protocol, known as the CEDAR for deciding paths [13], uses the central node of the network. This is a major drawback of this protocol that when a core node is destroyed, too much money will be needed to restore a core node. Since there are many data transfers in the WSN architecture, no core node is needed. The key TDMA-based routing protocols proposed by authors Lin [14] and Zhu et al. [16] will create a route with a reserved bandwidth taking into account QS from source to destination. This bandwidth measurement is done hop by hop.

The SSR protocol in [16] is the only network sensor protocol which comprises idea of QoS. The trees were routed from sink 's neighbor in this protocol and are used as a hop. This takes into account the QoS parameter for every hop, including each track energy resource and each packet's priorities. Later, by using the trees generated, several paths are built from sink to sensors. Therefore, one route can be chosen depend on the accessibility of energy resources and QoS. However, this approach to SAR is overloaded by holding the node states on each node of sensors.

In [17, 18] the authors show that the efficiency of sensor nodes can be enhanced with better resources. The sensor nodes perceive the most energy-efficient environment, scaling, and reliability by providing the cluster heads in each cluster [19].

III. Proposed System

The protection of a wireless network is the key concern and sinkhole attacks are so intense that no other attacks will withstand them. Security efforts have been channelled to explore the possibilities of sinkhole attack on a LEACH sensor network to boost attack impact and IDS to minimize harmful effects as a routing protocol.

3.1 Launching of Sinkhole Attack:

Attacks are categorized into two different forms of attack. The initial launch is to start a coordinated sinkhole attack with a set of CH nodes. The goal is to compromise the network-wide 'nc' nodes, so that the cluster contains any compromised node. The number of clusters in a collective sinkhole attack is the same as the number of compromise nodes. Thus, normal sensor nodes monitor the affected nodes to project their energy values into CH above threshold. Usual nodes send their data packets to the constantly disabled CHs, allowing any CH or sinkhole nodes affected to drop or exploit their systems to make sure the safety violations are fulfilled. A compromise lockout attack will be launched to manage the data of its cluster members within network. For every round of selection procedure CH is compromise rather than compromise the "nc" cluster to launch the sinkhole attack.

In such a situation one CH would be malicious to act like a sinkhole. Although the performance of each transmission of data is limited, in the compromised sinkhole attack the malicious activity was further extended. Issue of sensor networks was therefore tackled as a challenge. However, the IDS mechanism can effectively detect such attacks.

3.2 Algorithm: IDS Algorithm for Sinkhole Attack

Begin

S_n is the sensor network and PTi be the total packets transmitted by the i^{th} CH in S_n

PR_i is the total packets received by the i^{th} CH in S_n

N_i is the Cluster head Node ID

P_i is the Intrusion ratio for the i^{th} CH

Repeat

Time delay (100)

For $\forall$ (C_i)

Receive (PR_i, PT_i and N_i) packets from the CHs'

Calculate P_i where $P_i = PR_i/PT_i$

If P_i tends to∞then

Corresponding N_i is the sinkhole node

Isolate N_i

Send warning message to the remaining cluster member nodes about N_i

Else

Corresponding N_i is the normal CH

End if

End for

Until the nodes transmission process completes

End

3.3 Algorithm Description:

IDS Agent module runs through BS toward identify intrusion by analyzing PRi , PTi, and $N\ i$ data packets on a regular basis. The intrusion ratios (IR), whether or not numerical, are checked by the IDS agent by the packet transmission value of CH (PTi), packet reception value of CH (PRi), with CH node recognition Ch ($N\ i$). When PRi to PTi ratio is numeric, packet does not drop to ensure "there is no malicious activity." If not, the corresponding CH (IR is infinity) is a sinkhole node that lost any data packet that resulted in a black hole attack. On other hand if the PRi and PTi values vary widely, a selective forwarding attack can be feasible.

Above technique was intended toward reduce intrusion ratio so that in next round of data transmission the attacker node can be separated and removed by the BS from CH selection process. Proposed mechanism for IDS tells individual members of the cluster that a sinkhole node is present to avoid the further communication of data. In addition, the calculation of the sinkhole-node is much reduced by the local information available and the power efficiency of the networks is also enhanced with rapid recognition of affected nodes. Given that the IDS system proposed has less overall coordination among the sensor networks with BS, calculation of a ratio gage was easy to facilitate calculations that further reduce computational complexity. Even with an increased node density, the proposed IDS method alerts the risk deduction efficiently.

IV. Results and Discussion

4.1 Simulation Description:

The NS-2.35 simulator is used for our experiments. We carry out two steps of the experiments. The first step is to test our plan 's feasibility and then investigate in greater depth in order to assess delays and performance.

In the first step, the network comprises 30 mobile nodes, and communication begins from source to goal. Here hop to hop contact takes place and the distance depend on position of a single node was determined. Numbers of data flows calculated for individual user to user communication. The transmission rate for each node dependent on pheromone values can be

defined here. In our work we can retain energy and delay for each node and find the perfect path to pick a route.

We use 25 nodes in the 4-cluster network, which uses CBR as application traffic with the rate of transmission of 1024 packets/0.5ms. The networks are Area-1000X1000 and are 250 m in the radio-range, random topology, with two-way soil as propagation model. We use 100000 maximum packets, routing methods are QOS-MRP or MSHA-IDS. The simulation time is 10000ms, initial energy-100j and AODV as a routing protocol.

4.2 Simulation Table:

PARAMETER	**VALUE**
Application Traffic	CBR
Transmission rate	1024 packets/0.5ms
Radio range	250m
Topology	Random
Propagation model	Two way ground
Packet size	1024 bytes
Maximum speed	20m/s
Simulation time	10000ms
Number of nodes	30
Area	1000x1000
Clusters	4
Initial energy	100j
Routing protocol	AODV
Maximum packets	10000
Routing Methods	QOS-MRP, MSHA-IDS

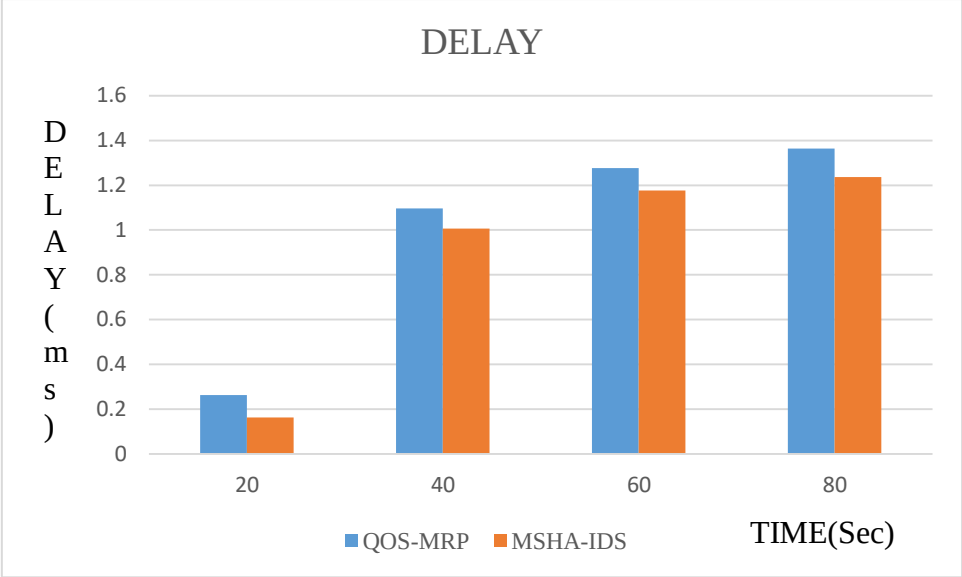

Figure 1: End-to-End Delay

Network delay was viewed in Figure 1. Delay in our system should be small compared with current approaches to achieve a better network efficiency.

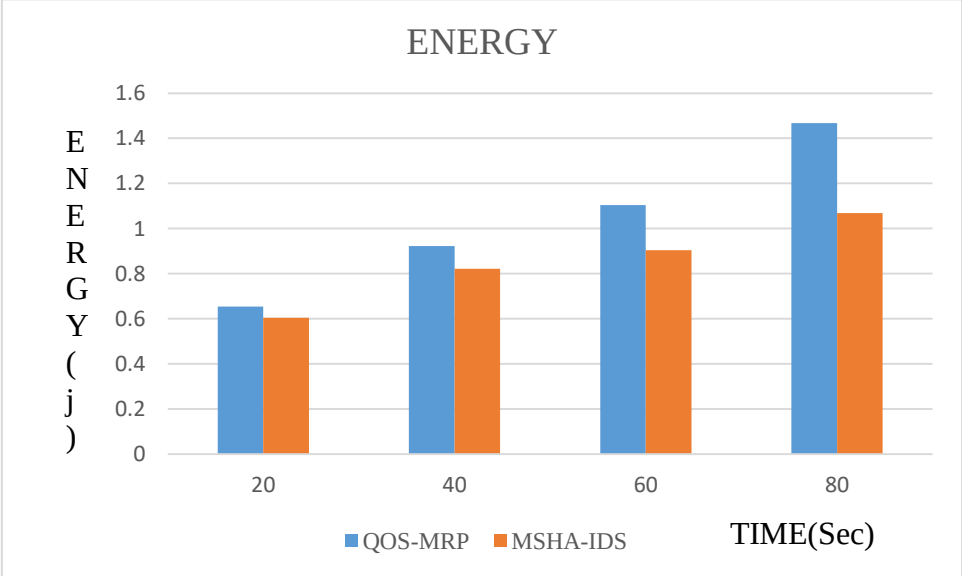

Figure 2: Energy Consumption

The energy usage of the network was given in figure 2. Energy consumption of our proposed system should be low compared with existing methods to achieve improved network efficiency.

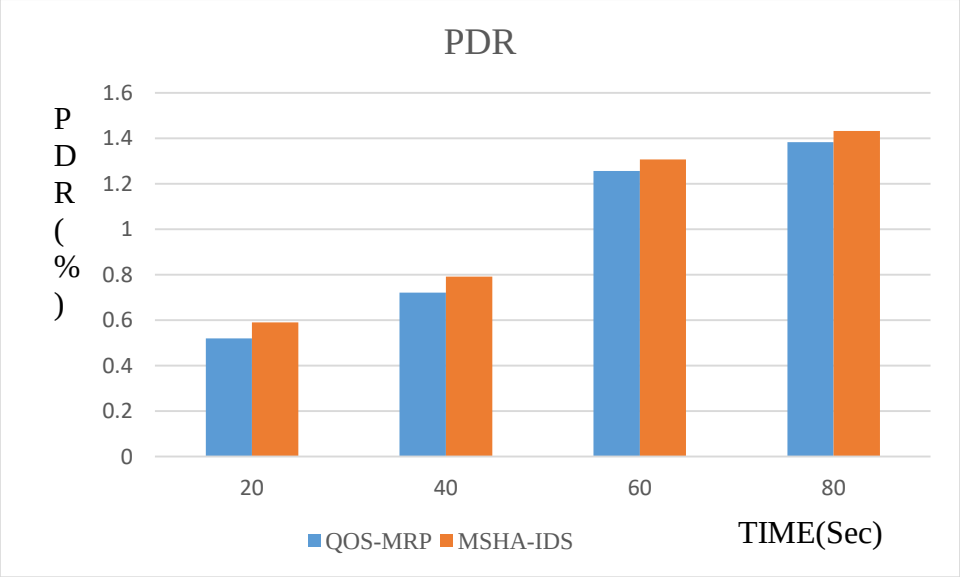

Figure 3: Packet Delivery Ratio

Figure 3 displays PDR (Packet Delivery Ratio). Packet Delivery Ratio in our proposed framework was high in comparison to current systems, in order to achieve improved network efficiency.

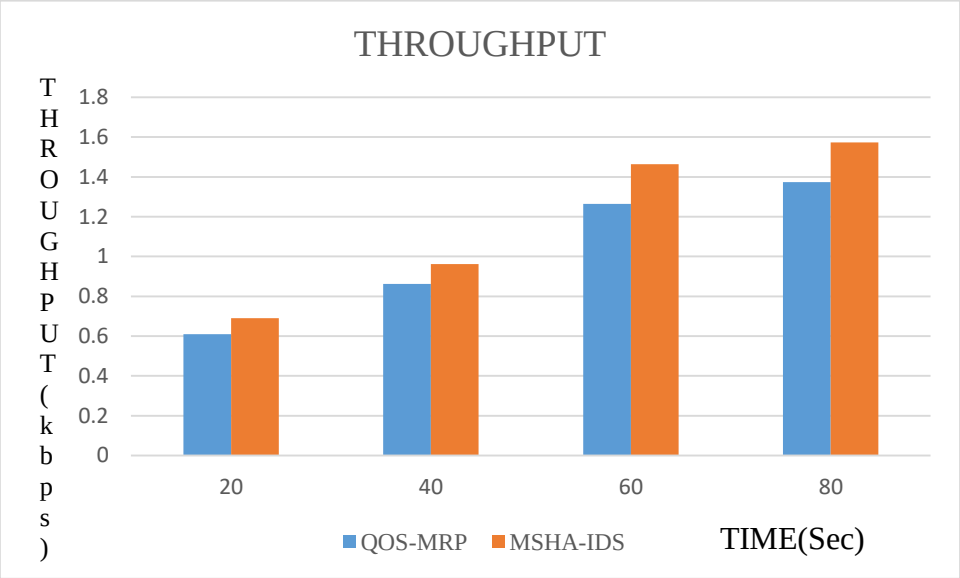

Figure 4: Throughput

The network efficiency is shown in figure 4. To attain better network performance, the performance of our proposed system should be high compared to current methods.

Conclusion

If an interruption takes place, sensor network output was improved through considering every QoS parameters. The routing multipath protocol is used to measure all routes from source to destination. WSN's like sinkhole assault are easily vulnerable to cyber threats. Thus, the IDS mechanism defining the LEACH protocol attacks with disturbing usual sensor node toward the rate of data loss is proposed. For analyses where sinkhole attack and IDS have been initiated, the NS-2 simulator is used. The results of the simulation show that the weakness of sinkhole attacks on LEACH drops every packets transmitted across CH. As computing proposed IDS is easy, energy consumption is lower, minimum latency, and the delivery ratio is higher. In contrast with the current mission, the network efficiency can be improved, namely QoS-MRP. For addition, it is possible to expand the proposed algorithm to detect a Selective Transmitting Attack that changes data fragments or a snooze attack.

References

[1] Abdullah Bamatraf, Mohammad Shafie Bin and Yahaya; Review of Quality of Service in Routing Protocols for Wireless Sensor Network, Journal of Theoretical and Applied Information Technology Vol. 74, No.3, April 2015, pp.310.

[2] Deris tiawan, Abdul Hanan Abdullah, Mohd. Yazid dris, “Characterizing Network Intrusion Prevention System”, International Journal of Computer Applications (0975 – 8887), Volume 14– No.1, (January 2011).

[3] K. Akkaya and M. Younis, A Survey on Routing Protocols for Wireless Sensor Networks. Ad Hoc Networks 2015, pp. 325349.

[4] S. K. Singh, M. P. Singh and D. K. Singh; Routing Protocols in Wireless Sensor Networks – A Survey. International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.2, November 2012, pp. 63-83.

[5] G. Kalnoor and J. Agarkhed, "QoS based multipath routing for intrusion detection of sinkhole attack in wireless sensor networks," *2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT)*, Nagercoil, 2016, pp. 1-6, doi: 10.1109/ICCPCT.2016.7530341.

[6] K. Pradeepa, W.R. Anne, and S. Duraisamy, “Design and Implementation Issues of Clustering in Wireless Sensor Networks,” Int’l J. Computer Applications, vol. 47, no. 11, pp. 23-28, 2012.

[7] S. Chen and K. Nahrstedt, “Distributed Quality-of-Service Routing in adhoc Networks,” IEEE Journal on Selected areas in Communications, Vol. 17, No. 8, August 2013.

[8] R. Sivakumar, P. Sinha and V. Bharghavan, “Core extraction distributed ad hoc routing (CEDAR) specification,” IETF Internet draft draft-ietf-manetcedar-spec-00.txt, 2014.

[9] C. R. Lin, “On Demand QoS routing in Multihop Mobile Networks,” IEICE Transactions on Communications, July 2010.

[10] C. Zhu and M. S. Corson, “QoS routing for mobile ad hoc networks,” In the Proceedings of IEEE INFOCOM, 2012.

[11] W. C. Lee, M. G. Hluchyi and P. A. Humblet, "Routing Subject to Quality of Service Constraints Integrated Communication Networks," IEEE Network, July/Aug. 2014.

[12] Z. Wang and J. Crowcraft, "QoS-based Routing for Supporting Resource Reservation," IEEE Journal on Selected Area of Communications, Sept 2013.

[13] Gajendra Singh Chandel, Ravindra Gupta and Arvinda Kushwaha, " Implementation of Shortest Path in Packet Switching Network Using Genetic Algorithm", in International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X , Volume 2, Issue 2, February 2012.

[14] N A. S. Alwan, I K. Ibraheem &, S M. Shukr, "Fast Computation of the Shortest Path Problem through Simultaneous Forward and Backward Systolic Dynamic Programming " in International Journal of Computer Applications, ISSN:0975 – 8887, Volume 54– No.1, September 2012.

[15] Ahmad Najari Alamuti, "SPAR: Shortest Path Adaptive Routing for Wireless Sensor and Actor Networks", in Darolfonoon Private High Educational Institute, Qazvin, Iran.

[16] Ali Norouzi1, Faezeh Sadat Babamir, Abdul Halim Zaim, "A Novel Energy Efficient Routing Protocol in Wireless Sensor Networks", in Scientific Research Journal of Wireless Sensor Network, doi:10.4236/wsn.2011.310038, 2011.

[17] N.Pushpalatha and B.Anuradha, "A Comparative Analysis of WSN Sensors Positioning Method using Iterative Routing Algorithm with Conventional Methods" in International Journal of Computer Applications, ISSN:0975 – 8887, Volume 53– No.7, September 2012.

[18] Onur Yilmaz and Kayhan Erciyes, "Distributed Weighted Node Shortest Path Routing for Wireless Sensor Networks", in University of Economics, Computer Eng. Dept., Balcova, Izmir, Turkey.

[19] I. R. Chen, A. P. Speer, and M. Eltoweissy, "Adaptive fault-tolerant QoS control algorithms for maximizing system lifetime of query-based wireless sensor networks," IEEE Trans. Dependable Secure Computing, vol. 8, no. 2, pp. 161– 176, 2011.

