IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Wireless Body Area Network, an Adaptive Energy Efficient MAC Protocol for Increasing Sensor Node Life

Nagashetty B Kolar

Scholar CMRU Bangalore

Dr S Saravana Kumar

Professor CMRU Bangalore

Abstract: Individual nodes in a wireless sensor network can interact with the physical environment statically or dynamically by sensing or manipulating physical parameters. In several critical applications, such as intrusion detection, target tracking, and industrial automation, wireless sensor networks have emerged as a prominent option. One of the most difficult aspects of WSN is determining the most efficient procedure for preserving power source energy. One of the primary difficulties in wireless sensor networks is the creation of an energy-efficient Medium Access Control (MAC) protocol (WSN). In this work, we look at certain WSN properties that are relevant for the design of MAC layer protocols, as well as a brief overview of some recently developed MAC protocols with regard to WSN energy efficiency. MAC protocols are grouped into four types based on channel access policies: cross layer protocols, TDMA-based, contention-based, and hybrid, which are covered in this work.

Keywords: **Mobile computing, Energy.**

1. Introduction

A Wireless Sensor Network is a network made up of several sensor networks that sense the environment, collect data, process it, and then send it over radio waves. WSN's most basic function is to sample and acquire data at the base station, but it can also conduct in-network processing tasks including event aggregation, actuation, and detection. The technology promised in the early WSN papers might be used for a wide range of monitoring applications, including waterways, forests, security, buildings, and war operations. The sensor node is inexpensive, but its transmission range is limited; as a result, the network is congested. When regular communication is occurring, the sensor node is energy efficient; however, when data is broadcast from the sensor node, the sensor node's life is reduced from one year to one month.

Data transmitted by sensor nodes is exposed to threats if the transmission channel is insecure, and data might be lost if a backup is not established in the event of a power outage. In this research, we will use data aggregation and data fusion approaches to improve the energy efficiency of a mote. We're also utilising encryption to safeguard the channel, as well as creating a backup of the data on the gateway and detecting an intrusion using sinkhole mitigation. One of the most important aspects of a Wireless Sensor Network is that It's important to keep in mind how effective the sensor can be. network. In a wireless sensor network, each mote delivers data. The data is subsequently sent to the base from the cluster head station. When the sensor nodes are separated by a significant distance during transmission, additional energy is consumed from each other. and when the mote transmits directly to the base It may result in erratic energy usage at the station. a group of people The number of mote in a sensor network is referred to as a cluster. In the event that the If the network is particularly vast, the motes will be clustered into distinct groups. Depending on the data to be perceived, groups or clusters are formed. Selecting a channel head first and then establishing the cluster is one of the best ways to create a cluster. Hierarchical Architecture is defined in [6] as the division of nodes depending on their hierarchy. The base stations are at the top of the hierarchy, while the sensing nodes are at the bottom.

2. Problem Statement:

One of the most serious issues in wireless data transmission is the presence of malicious nodes or attackers, which can lead to data manipulation or loss. In this paper, we propose an algorithm that assists in detecting malicious nodes or attacks on our system by detecting an intrusion and mitigating sinkhole nodes for secure data transmission from sensor nodes to base stations.

3. Types of Security Attacks:

a) Sybil Attack: A malicious node may be present in a peer-to-peer network to act as a distinct node in a Sybil attack. The rogue node may not pass the data received during communication or may act maliciously after entering the network. As a result, the network's quality and long-term viability suffer.

b) Selective Forwarding: In Selective Forwarding, some phoney or malicious nodes may drop data, preventing it from being transferred further, resulting in incomplete data transfer.

c) Sink Hole: One of the most common attacks involves a false node attracting data from its neighbour by acting as the shortest link between the node and the server or base station.

d) HELLO Flood Attacks: In the AODV Protocol, HELLO messages are delivered to neighbours to let them know that the node is in their transmission range, but an attacker can sometimes broadcast HELLO messages on a high quality range to trick other nodes into thinking it is their transmission range.

e) Dos Attack: A Dos Attack prevents a legitimate user from accessing data. The attackers flood the system with queries, preventing it from responding to legitimate users. This renders the system inaccessible to authorised users.

f) Node Replication Attack: A node replication attack is a type of attack that is not dependent on the application. In this attack, the malicious node builds its own commodity sensor node with its own hardware and then joins the network to accept it as legitimate.

g) Wormhole Attack: In a wormhole attack, the attackers record packets at one network site, send them to another location, and then retransmit them back into the original network.

4. Results and Discussion:

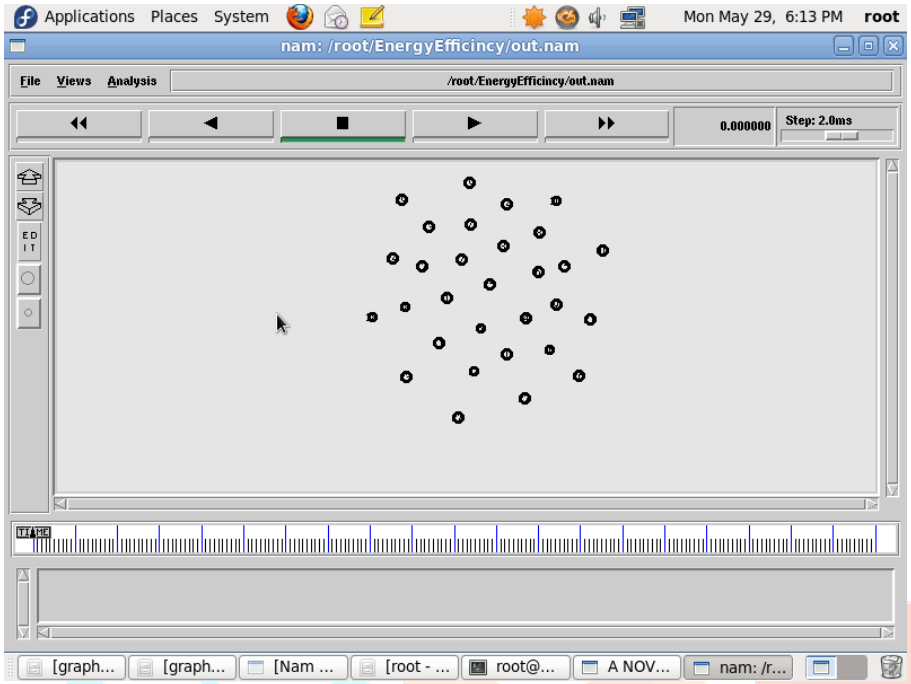

Fig 4.1 Simulation ork

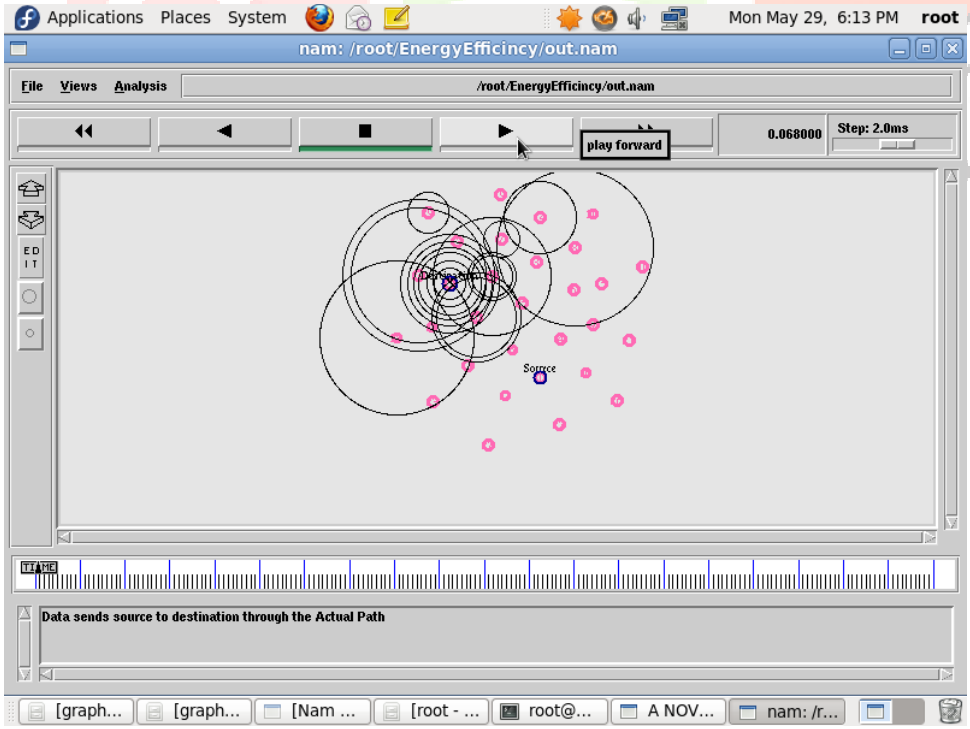

Fig 4.2 Data Communication

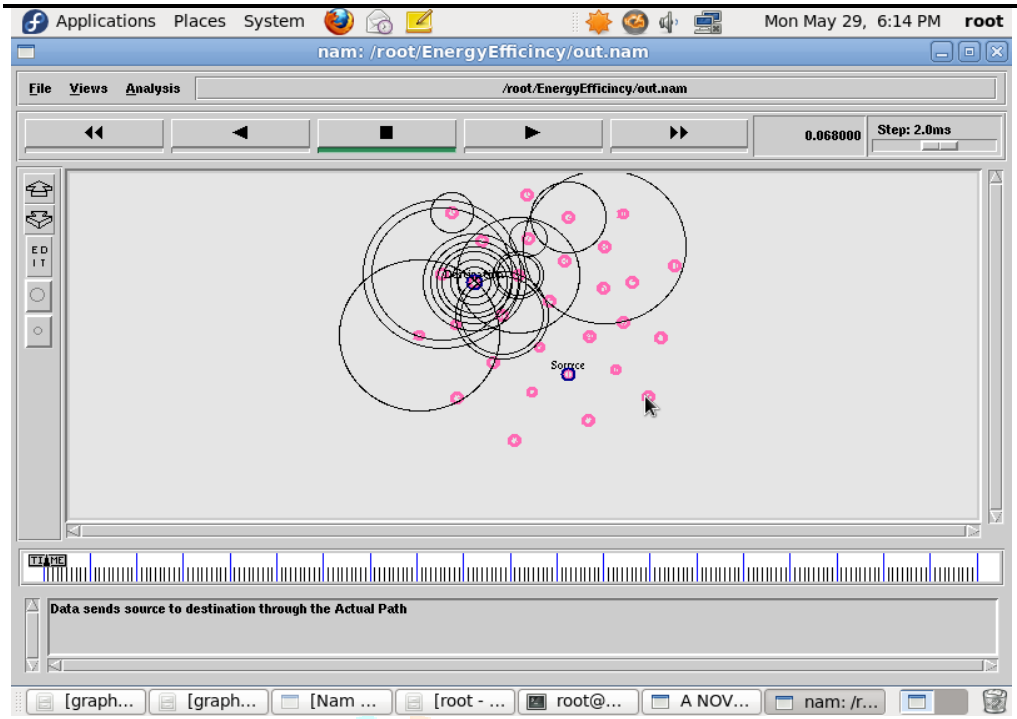

Fig 4.3 Initial and destination node setup

No. of Nodes	100
Area	600 X 600
MAC	802.11
Simulation Time	50 sec
Traffic Source	CBR
Rate	100Kb
Propagation	Two Ray Ground
Antenna	Omni Antenna
Initial Energy	8.1J
Transmission Power	0.650
Receiving Power	0.385

Performance Table

5. Conclusion

The architecture and protocol for implementing a smart cooling monitoring system are described in this work. Our research focuses on data transfer and detecting threats that may occur while data is being transmitted. We are identifying and correcting intrusion attacks on our network. We present a framework to handle the acquired sensory data in this paper, which focuses on the sensory data processing component of integrated WSN–MCC. We employed WBAN to improve the efficiency of the system, which helps to reduce packet loss and transmission latency. In the sensor gateway, the architecture contains data flow monitoring, prediction, filtering, compression, and decompression capabilities. Data encryption and decryption techniques are used in the sensor to boost the gateway's capacity. By simulating the intrusion effect and the effect of flooding attack using the network simulator NS2 and applying the proposed algorithm to lessen its effect, we were able to detect the intrusion effect and the effect of flooding attack in this study. It also demonstrated that the system is aware of the attack and that an algorithm is being used to mitigate the impact on the network.

Acknowledgment

The authors would like to thank a great support of

References

[1] Cheng, Chi-Tsun, Chi K. Tse, and Francis Lau. "A delay-aware data collection network structure for wireless sensor networks." Sensors Journal, IEEE 11.3 (2011): 699-710.

[2] Younis, Mohamed, and Kemal Akkaya. "Strategies and techniques for node placement in wireless sensor networks: A survey." Ad Hoc Networks 6.4 (2008): 621-655.

[3] Du, Kemei, Jie Wu, and Dan Zhou. "Chain-based protocols for data broadcasting and gathering in the sensor networks." Parallel and Distributed Processing Symposium, 2003. Proceedings. International. IEEE, 2003.

[4] Khaleghi, Bahador, et al. "Multisensor data fusion: A review of the state-of-the-art." Information Fusion 14.1 (2013): 28-44.

[5] Akyildiz, Ian F., Tommaso Melodia, and Kaushik R. Chowdhury. "A survey on wireless multimedia sensor networks." Computer networks 51.4 (2007): 921-960.

[6] Rajeshwari, P., B. Shanthini, and Mini Prince. "Hierarchical Energy Efficient Clustering Algorithm for WSN." (2015).

[7] Nithyakalyani, S., and B. Gopinath. "Analysis of Node Clustering Algorithms on Data Aggregation in Wireless Sensor Network." Journal of Scientific & Industrial Research 74.1 (2015): 38-42.

[8] KALAISELVI, G., G. Kalaiselvi, and D. Anitha. "Energy Efficient Data Aggregation Using Packet Driven Timing Algorithm in Wireless Sensor Network." International Journal for Innovative Research in Science and Technology 1.9 (2015): 107-111.

[9] Singh, Shio Kumar, 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 (2010): 63-83.

[10] Liu, Yun, Qing-An Zeng, and Ying-Hong Wang. "Energy-Efficient Data Fusion Technique and Applications in Wireless Sensor Networks." Journal of Sensors 501 (2015): 903981.