Control of Selfish Attack using Selfish Mac Protocol

J BabithaRani[1], K.SureshBabu[2],
[1]*PG Scholar*, [2]*Associate Professor*,
[12]*Department of Computer Science & Engineering, JNTUH School of Information Technology*

Abstract- The WSN played the important role in improving the life of the people in several fields such as health, industry, surveillance, environment-monitoring, battle etc. For the last few years, the population of aged persons has been increasing worldwide. A traditional medical care system use stationary wired medical apparatus which are inconvenient and have a higher impact on the standards of living of patients and involves a high cost of implementation and maintenance. While diagnosing these diseases doctors face difficulties in early detection and long observation of diseases. To overcome these problems a new monitoring system is emerged as Wireless Body Area Network (WBAN).Medium Access Control (MAC) sub-layer faces more challenges as compared with other layers because of radio that consumes more energy resources. Thus, any possible attack over the MAC makes the slowdown working process of WBANs. There are several well-known attacks that cause the additional energy consumption observed at the MAC layer in WBANs. These attacks involve the collision and selfish attack. The collision attack and denial of sleep attacks are researched and handled for MAC over the WBANs. However, selfish attack is not properly addressed. In this paper, we propose a selfish detection medium access control (SDMAC) algorithm against selfish attack in WBAN. To validate the performance of the proposed algorithm, the simulation is conducted using NS2. Based on the simulation results, we demonstrate that our proposed SDMAC outperforms other known existing protocols from energy efficiency.

Keywords-Wireless body area network (WBANs), selfish attack, and energy consumption.

I. INTRODUCTION

Wireless networks provide unprecedented freedom and mobility for a growing number of laptop and PDA users which no longer need wires to stay connected with their workplace and the Internet. Ironically, the very devices that provide wireless service to these clients need lots of wiring themselves to connect to private networks and the internet.For the last few years, the population of aged persons has been increasing worldwide. A traditional medical care system use stationary wired medical apparatus which are inconvenient and have a higher impact on the standards of living of patients and involves a high cost of implementation and maintenance. While diagnosing these diseases doctors face difficulties in early detection and long observation of diseases. To overcome these problems a new monitoring system is emerged as Wireless Body Area Network (WBAN). A WBAN consists of small and intelligent sensors which are either placed on or with in human body.These sensors monitor body conditions and a leader collects this information and sends them to concerned healthcare Centre. During this process of transmitting the data from the leader, the WBAN faces energy exhausting attacks such as collision and selfish. These attacks reduce the lifetime of the sensors and compromise the WBAN, which results in decrease in the quality of healthcare.Since we are dealing with the human life, these energy consumption attacks must be addressed.In this paper a genetic algorithm is proposed to mitigate selfish attack by detecting selfish node and blocking unusual activities.

The remaining paper is organized as follows. Section II explains the related work done in the field, Section III discusses the proposed SDMAC protocol, the Simulation Setup and Results are discussed in section IV and the paper is concluded in Section V.

II. RELATED WORK

Wireless Body Area Network (WBAN):

A WBAN (Wireless body area network) is a wireless network of the wearable computing device. These devices may be placed in the human body or surface mounted on the human body in a particular position. The growth of attention in wearable technologies such as glasses, watches has meant an improved focus on wireless networking. The term WBAN (Wireless body area networks) have been invented to refer to the wireless network technology used in combination with wearable's. The main purpose of these networks is to transmit data produced by wearable devices at outside to a WLAN or the Internet. In some cases, wearable's can also exchange the data directly with each other. As we all know that, researchers are implementing the new and advanced technology in the field of science. Various kinds of the networks or sensors are introduced in the networking field, which are used to monitor the traffic, health in a simple way. As a result of this technology many researchers has been invented a new technology that is called as the BAN or sensor that allow us to monitor the inside activities like chronic diseases.The field of a BAN is a particular area which could permit cheap and constant health monitoring medical records through the Internet. A Number of intelligent physiological sensors can be combined into a wearable WBAN (wireless body area network), which can be used to detect medical conditions. This area relies on the viability of implanting very small bio

sensors inside of the human body. The fixed sensors in the human body will gather various physiological variations in order to observe the status of the patient's health.

Challenges of WBAN

WBAN has also faced various challenges in the competition of various technologies. The different challenges of WBAN include

- The different sensor devices are used in the formation of the WBAN and the construction of complex nature sand is very difficult.
- Many people think that this WBAN technology is not safe in the field of hospitality as equated to other medical devices.

When the WBAN's are used for the data transmission they are not beneficial and can intrude the transmission of data & decrease the efficiency.

Drawbacks:

- WBAN faces energy exhausting attacks such as collision, denial of sleep, and selfish.
- Due to selfish attacks the nodes does not participating in Route Discovery Phase then packet forwarding function will never execute.
- These attacks reduce the lifetime of the sensors and compromise the WBAN, which results in decrease in the quality of healthcare.

III. SDMAC

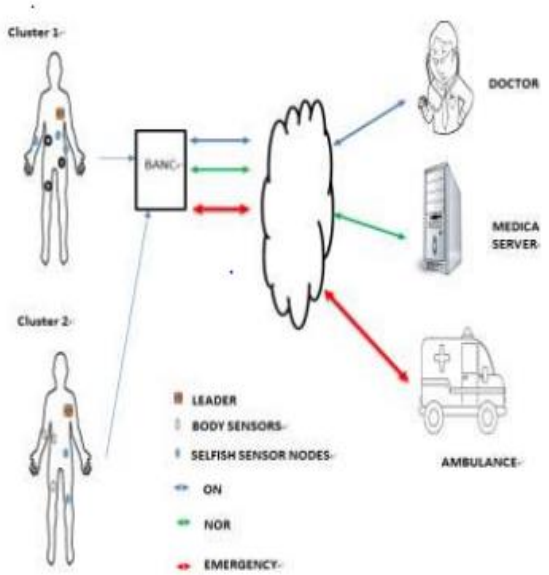
Selfish detection media access control Protocol (SDMAC):

Selfish detection medium access control (SDMAC) algorithm against selfish attack in WBAN. Here the adversary nodes have advantage over legitimate nodes on MAC protocols that use the resources wrongly, which leads to energy consumption in sensor nodes, proposed algorithm detects the fake node and blocks the unusual activities. This protocol detects the selfish attack in the wireless body area networks and prevents the selfish nodes from exploiting the network. This is done by estimating the trust calculation of each senor node. If the trust calculation value of any node is less than a set threshold then the node is considered to be malicious and thereafter the node is blocked by the network.Medium Access Control (MAC) sub-layer faces more challenges as compared with other layers because of radio that consumes more energy resources.

This section discusses the proposed SBMAC scheme by dividing it into two parts. (A) System model and (B) Selfish detection media access control protocol.

A.System model:

The system model for the Wireless body Area Network. Here the clusters represent the host body which has to be monitored by the Medical personnel. The human body is placed all over with the sensor nodes in it. These sensor nodes are accompanied by the leader node and actor node which is able to communicate with the all nodes and the outside network. All the other normal nodes are supposed to be communicating with only leader node through actor node. The actor is supposed to control the traffic from the normal nodes. These sensors in the body read the status of the patient and report to the leader node. Leader node keeps the track of information and sends to BANC (Body Area Network Coordinator) which sends all information to medical personnel using internet which can be wired or wireless. Wireless is preferred more for its flexibility and convenience of the patients and personnel.



This BANC helps in monitoring according to the situation of the patient. If the patient needs an urgent medication and to be hospitalized immediately it sends information to the emergency services who can handle the situation of the patient. It sends information to doctor for some required situations and irregularity behavior. It constantly sends information to the personnel where the patient conditions can be saved in the medical server. By this model a patient can be monitored all the time and can be taken good care.

Assumptions for leader node:

In this sensor nodes leader is selected in body area network has to behave heterogeneously. Heterogeneous node have many advantages in its own way that are prolonging the lifetime of the network, improves the reliability of the data transmission and decreases the latency of the data transportation.

B. Mathematical model

T - over all lifetime of network

Ts - Constant rate of success

Tf - constant rate of failure

Pn – probability of node to be normal

Ps – probability of node to be selfish

Let us define Q random variable as

Q = 0; if nodes are normal

Q=1; if nodes behaviour is selfish during route discovery

Q=2; if nodes behaviour is selfish during route reply

Q=3; if nodes behaviour is selfish during data rely

Let M be residual lifetime of node existing in selfish node Let N1 and N2 be the time to failure of normal and selfish nodes Probability mass function of Q be

$P_Q(0) = Ts(1 - Pf)/(Ts + Tf)$

$P_Q(1) = TsPn/(Ts + Tf)$

$P_Q(2) = Ts(1 – Ps)/(Ts + Tf)$

$P_Q(3) = Tf\ Ps/(Ts + Tf)$

Lifetime of node is given by min (N1, N2) + M N1, N2 are exponentially distributed with parameter Ts + Tf Conditional success of node in normal node is given by

$L_{T/Q}(S/Q = 0) = (Ts + Tf)/(S+Ts + Tf) = L_{T/Q}(S/Q = 2)$

Conditional success of node in selfish mode either in route discovery or in route reply.

$L_{T/Q}(S/Q = 1) = (Ts + Tf)/(S+Ts + Tf) * (Ts)/(S+Ts) = L_{T/Q}(S/Q = 3)$

Total transform

$L_{T/Q}(S) = (Ts + Tf)/(S+Ts + Tf)\ \{(TsPn+ TfPS)/(Ts + Tf) * (Ts)/(S+Ts) + (Ts(1-Pn) + Tf(1-PS))/(Ts + Tf)\}$

Conditional success rate of network

$L_{Q1}(S) = (Ts + Tf)/(S+Ts + Tf)\ L_{Q2}(S) = (P\ Ts)/(S+Ts) * (1-P)$

Total probability at which the node could be either in normal node or selfish node

$P = (TsPn+ TfPS)/(Ts + Tf)$

Conditional success of node

$FX(t) = (1-P)(Ts + Tf)\ e^{-(Ts+Tf)*t} + P/Tf\ [(Ts + Tf)\ e^{-(Ts*t)} - Ts\ e^{-(Ts+Tf)*t}]$

C. Selfish detection media access control protocol

In order to detect the selfish attacks in wireless body area networks we propose Algorithm 1.The algorithm 1 explains the procedure of Selfish attack detection by HSA. All the Nodes send Route Request (RREQ) to Leader which is acknowledged by the leader node in the form of Route Response (RRES). Step 1 initializes the parameters used in the algorithm. The RREQ and RRES handshake done by the leader node and neighbour node happens in Step 2 and Step 3. In step 4, the Information about the neighbour nodes Energy (E), Packet Count (P), and Queue Size (Q) is acquired by the leader. A report is then generated and the trust value (Tc) is calculated in the next step. If the Trust value is more than 0.65, then the node is detected as a selfish node and blocked right away. In step 11, if the value of Tc is less than 0.65 then the node is taken as legitimate and data transfer through the node takes place.

Algorithm 1: Selfish detection media access control Protocol (SDMAC)

1. Initialize parameters (D:Data, RREQ: Route request, Route Response E: Energy consumed, P: Packet Count, Q: Queue size, Tc: Trust Calculation, p: integer > 0, P: Packet count, ts: Time for success, t: time transactions ≥ 0, K: Blocked node Constant = 1)
2. Read RREQ *\ RREQ from Node "N"
3. Send RRES *\ RRES to Node "N"
4. Read E, P, Q information *\ Neighbour Node "N"
5. Assign Tc = ts + (p/2) / (t+P)
6. Calculate Tc
7. If Tc > 0.65 then
8. Assign Blocked node k ← Node N
9. K ← K + 1
10. Else if
11. Tc ≤ 0.65 then
12. Send D *\ Node is legitimate
13. End if

End else if

III. SIMULATION AND RESULTS

In this section, we measure the performance of our proposed approach selfish detection medium access control (SDMAC) algorithm and compared with known body area network medium access supported protocols: IEEE 802.15.4 on is conducted using network simulator (NS2) and Ubuntu 12.10 operating system. The network consists of 500 X 500 square meters that involves 50 nodes. Furthermore, we also generated 2 malicious nodes.

Add results here

IV. CONCLUSION

In this paper a new scheme, Selfish Detection Medium Access Control Protocol, is proposed. This protocol detects the selfish attack in the wireless body area networks and prevents the selfish nodes from exploiting the network. This is done by estimating the trust calculation of each senor node. If the trust calculation value of any node is less than a set threshold then the node is considered to be malicious and thereafter the node is blocked by the network. A series of simulation tests have been carried out using NS3. The results demonstrate that our proposed approach outperforms with IEEE802.15.4 in the form of Bandwidth reduction and Energy consumption.

V. REFERENCES

[1]. "Detection of Selfish Attack over Wireless Body Area Networks" IEEE Open Systems (ICOS), 2017, Miri, Sarawak, Malaysia.

[2]. Razaque, Abdul, and Khaled M. Elleithy. "Energy-efficient boarder node medium access control protocol for wireless sensor networks." Sensors 14, no. 3 (2014): 5074-5117.

[3]. Razaque, Abdul, and Khaled M. Elleithy. "Low duty cycle, energyefficient and mobility-based boarder node—MAC hybrid protocol for wireless sensor networks." Journal of Signal Processing Systems 81, no. 2 (2015): 265-284.

[4]. Wang, Changhong, Qiang Wang, and Shunzhong Shi. "A distributed wireless body area network for medical supervision." In Instrumentation and Measurement Technology Conference (I2MTC), 2012 IEEE International, pp. 2612-2616. IEEE, 2012.

[5]. Jo, Minho, Longzhe Han, Nguyen Duy Tan, and Hoh Peter In. "A survey: energy exhausting attacks in MAC protocols in WBANs." Telecommunication Systems 58, no. 2 (2015): 153164.