Intruder Attacks on Wireless Sensor Networks: A Soft Decision and Prevention Mechanism

Iftikhar Hussain[1]
School of Computer Science and Technology
University of Science and Technology of China
Hefei 230000 China

Abrar Hussain[3]
Hefei National Laboratory for Physical Science at the Microscale
University of Science and Technology of China
Hefei 230026 China

Shahzad Haider[5]
School of Electronics Science and Technology
University of Science and Technology of China
Hefei 230026 China

Samman Zahra[2]
Computer Science Department
COMSATS Islamabad
Islamabad 45550 Pakistan

Hayat Dino Bedru[4]
School of Software
Dalian University of Technology
Dalian 116620 China

Diana Gumzhacheva[6]
School of Management Science
Anhui University
Anhui 230031 China

***Abstract*—Because of the wide-ranging of applications in a variety of fields, such as medicine, environmental studies, robotics, warfare and security, and so forth, the research on wireless sensor networks (WSNs) has attracted much attention recently. WSNs offer economical, flexible, scalable and pragmatic solutions in many situations. Sensor nodes are tiny and have a limited, non-rechargeable battery source, small memory/computational abilities and low transmitter power. Energy resources are vital as once the battery is depleted, the node is no longer usable. Multiple medium access control (MAC) protocols are designed to increase the life cycle of a node by minimizing its unnecessary energy consumption. In some critical applications like the surveillance of enemy movements on a battlefield, opponents deploy adversary nodes to disturb the performance of WSNs by mainly depleting the battery sources of legitimate nodes. In this work, an intrusion detection mechanism has been adapted to detect different kinds of intruders' attacks in MAC protocols of WSN's. A soft decision mechanism has been implemented to detect collision and exhaustion attacks. A preventative mechanism has also been introduced, which helps a node to avoid these intrusive attacks. Results show how the lifetime of a node increases and network performance also increases with better throughput and reduced delay.**

Keywords*—MAC protocols; S-MAC; wireless sensor networks; intrusion detection

I. Introduction

Medium access controls (MAC) perform the key action of developing coordination among nodes and managing the means for their effective communications with the help of an allocated medium. There are various procedures formulations in different situations. Such designed procedures also differ for varying applications and constraints [1]. MAC is one of the major concerns when designing wireless sensor networks. Realizing the concern over limited energy resources encountered in the domain of wireless sensor networks, MAC protocols are exclusively designed in a way to render them energy efficient. One primary cause of excessive energy consumption or wastage is the transfer of data by the two nodes sharing the same medium at the same time [2]. This data transfer leads to the collision of the data packets. In order to accommodate this problem in sensor networks, the MAC procedures are expected to aid the nodes in accessing the medium to avoid the packets' collisions [3]. MAC procedures or protocols are significant features for running any network embodying a shared medium and for attaining efficient performance of the network. In the context of wireless networks, MACs are studied extensively in [4].

Wireless protocols, such as time division multiple access (TDMA), code division multiple access (CDMA), and frequency division multiple access (FDMA), are conventional and are usually employed in conventional wireless networks. Since sensor nodes are powered by battery, these protocols cannot be directly applied to wireless sensor networks [5]. Due to this limitation, such protocols have minimal memory as well as computation power. It is also due to this limitation of wireless protocols that MAC protocols cannot be directly applied to wireless sensor nodes, and this is why they need obligatory alteration [6]. In order to design efficient MAC protocols for sensor networks, network scalability and the computation of energy efficiency are the primary and essential considerations. Features such as latency, bandwidth utility, and throughput are of secondary importance. In a nut-shell [7], priorities and considerations differ with distinct applications of sensor networks.

The remainder of the paper is designed as follows: Section II will give a brief overview of all the terminologies that are used in this research article; Section III is dedicated to the description of some common network attacks on S-MAC, while Sections IV and V will explain the function and simulation results of our proposed detection mechanism.

II. Problem Description

A. Sensor Medium Access Control (S-MAC)

Sensor Medium Access Control is a MAC protocol for sensor networks that is energy efficient. The major applications of S-MAC include tolerance latency and long idle listening. S-MAC's communication occurs among nodes, which also act as each other peers, rather than as solo base stations [8]. In

addition to the maintenance of collision avoidance, it is equally important to adjust scalability to maintain or improve energy efficiency. S-MAC [9] achieves energy efficiency by reducing energy usage from every main source that is responsible for the excessive use of energy. In return, it permits partial performance degradation in both latency and per-hop fairness.

B. Synchronization in S-MAC

Synchronization mainly depends on all the three phases which includes:

- Listening period
- Wake-up period
- Sleep period

Following the standards of 802.11 IEEE, numerous efficient control methods such as sleeping, collision avoidance, synchronization, and listening are usually coupled with a contention-based MAC while implementing S-MAC. In principle, S-MAC employs a cyclic wake-up method wherein each node has its listening and sleeping period of the definite length according to its schedule [10]. In this method, every node switches to sleep mode for a defined period and then wakes up for subsequently fixed listening as shown in Fig. 1.

Listening Node - Listening mode is further broken down into three phases:

- SYNC phase
- RTS phase
- CTS phase

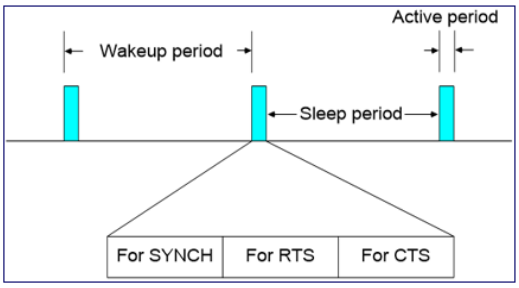

Fig. 1. Synchronization in S-MAC

Below is the description of each synchronization phase of S-MAC:

SYNC phase: In this type of phase, node A collects the transferred and corresponding packets from its adjacent B node and C node. It then generates a table of the listening periods of adjacent (A, B) nodes in a designed table. The A's SYNC stage is additionally separated into intervals of time [11]. When the adjacent node B is struggling to send a SYNC packet, it is picked at any given time, arbitrarily placed, and then begins the sending process in case no other signal is found in previous vacancies. If any signal is found, node B returns to sleep mode, and it waits in this mode until node A wakes up. In other words, A keeps count of B's timetable. It is possible for A to wake up for reasonable periods to send its SYNC data packet to B in the mode of broadcasting. This part is the synchronization.

Request to send (RTS) phase: Following synchronization, nodes start receiving transferred signals or packets from the adjacent nodes. RTS/CTS handshake is employed to avoid a signal collision.

Clear to send (CTS) phase: In this phase, CTS is transmitted upon receiving the RTS data packet from the adjacent nodes. Following this transmission is the beginning of the exchange of the packet, and this exchange continues for the optimum sleep time of A.

On synchronizing the schedules of A and its adjacent nodes, all nodes wake up at the same moment, and one and only one packet of SYNC is to be transmitted by A in order to reach all of its adjacent nodes. With the immense help of the S-MAC procedure, all the adjacent nodes reach an agreement on the same limited time table which then becomes the basis of shaping virtual clusters. The transmission of data packets [12] is not at all hindered by clustering as it only performs the exchange of schedules.

S-MAC protocols continue creating virtual clusters., Upon installing and switching, node A listens for a pre-defined and known synchronized time. If node A gets any SYNC packet from its adjacent nodes, say node B, it starts following its timetable and starts switching and transmitting packets the moment that node B enters into its listening period. Another scenario is that node A chooses a timetable for itself and starts transmission accordingly. In between the contention period of the transmission of the packet, if node A gets the timetable of any of its adjacent nodes, it strictly starts following it after dropping its schedule. If node A gets a signal that its adjacent nodes are following its schedule, then it prefers to stick to its schedule and, most likely, A will begin transmitting the data packets following both schedules. In this case, node A comes to know that neither of its adjacent nodes overlaps with its timetable, then it again starts following the timetable of its adjacent node and drops its own. However, node A always can get an invalid SYNC data packet and, in this case, it starts listening to its adjacent nodes to attain an entire synchronization period [13]. Due to this arrangement of virtual clusters, this instance is reasonably difficult.

The big multi-hop network is categorized into 'islands of timetable harmonization'. The nodes which are at the verge of a virtual cluster follow more than one timetable to forward their SYNC data packets. Hence, such nodes use more energy than the nodes with adjacent nodes of the identical timetable. Because of the cyclic wake-up method in S- MAC, the nodes spend most of their time in sleep mode which has a good reputation in terms of battery usage despite their latency. One of the major drawbacks of S- MAC is that it becomes quite challenging to catch up with the time duration while switching from the wake-up phase to the altering load states [14]. This is due to the limited time duration of the listening mode.

C. Timing Relationships in S-MAC

The scheduling is done by sending the SYNC packet, which is a small packet that contains sender information such as its address and its next sleep time. When the sender starts transmitting the SYNC packet, its next sleep time is related to that moment. After the reception of the SYNC packet, the receiver gets the time from it and subtracts this time from the

transmission time of the packet [13]. For the nodes which are to receive both the data and SYNC packet, the listening interval time is divided into two parts where the SYNC packet gets the first part, and the data packet gets the second part of the time interval, as Fig. 2 shows. There is a contention window for each part which has time slots for the sender to do virtual carrier sensing before transmitting. If the SYNC packet [14] is going to be transmitted, the sender has to do carrier sensing when the receiver begins listening.

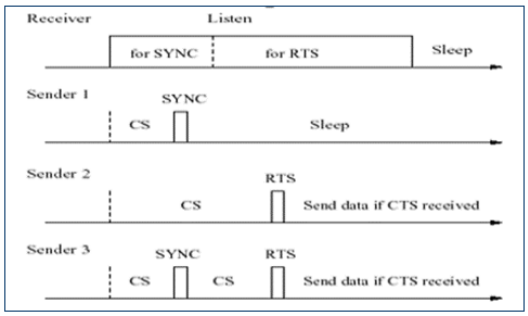

Fig. 2. Timing Relationship in S-MAC

1) The first part of the figure shows that sender 1 has done the carrier sensing and after getting access to the To end, the carrier sensing it selects any random time slot. If there is no transmission detected by the node at the end of the time slot that it got randomly, then it gets the contention window for the transmission of the SYNC packet and transmits the SYNC packet. Similarly, when the data packet is sending, the same procedure is adopted by the nodes. Fig. 2 shows three different scenarios in which there is communication between the sender and the receiver.
the channel, only the SYNC packet is sent for synchronization with the node.
2) In the second part of the figure, sender 2 has done the carrier sensing, sending the RTS packet and then the data packet if it received the CTS packet. It shows the transmission of a unicast packet.
3) The third part of the figure shows that sender 3 has done the carrier sensing and then sent the SYNC packet. After that, it again did the carrier sensing and sent the RTS packet. If it got the CTS packet, it would transmit the data packet. It shows the sending of both the SYNC and data packet.

III. Related Work

While talking about networks, with the recent advances in technology world Wireless Sensor Network (WSN) became one of the most capable network solution to most of the communication problems [29] that might be encountered in the field of Health, Military and Agriculture etc. It's obvious that there are two sides of a picture, along with this positive and promising side of WSN there is a weak and vulnerable side too. Because in WSN the involved sensor nodes are also vulnerable to some serious security attacks and the reasons vary from the gaps left in their deployments to some sensitive nodes that might be left unattended [30] because of being present in the areas where there is no one to properly check their security. Our article has also focused on some serious security attacks on WSN. Authors in [20] have also focused on one of the most occurring attacks on WSN i.e. DoS Jamming attack. This attack works by sending a huge volume of illegitimate traffic to the node in order to jam the legitimate traffic and thus the network. The technique proposed in this article exponentially weighted moving average (EWMA) is used to detect abnormal changes in the intensity of jamming attack. While the authors in [21] have studied the protocols related to access control in WSN. Their work has focused on the authentication problem during accessing the networks. They have analyzed different access control protocols and also include discussion on replacement of expensive protocols with some affordable ones. The article [22] discusses about the Intrusion Detection System (IDS) proposed for WSN. They have done a survey on different IDS for WSN and also for Mobile Ad-Hoc Networks (MANET). Lastly, they have proposed an IDS scheme for WSN after comparing the existing schemes along with their weaknesses. An Intrusion Detection System has been proposed in [23] for the detection of sinkhole attack in WSN. The article included the attack implementation to check their proposed IDS followed by the in depth study of Sinkhole attack. Another work done on a commonly occurring Worm attacks in WSN in [24] focusing specifically on prevention of the sensor worms from propagating in the entire network. They have proposed an algorithm for assigning the relevant version of software to each sensor node in the sensor network to restrain the worm propagation. Researchers in [25] have done an analysis of a number of different security issues related to data integrity, data availability and data confidentiality. They have analyzed different security attacks on WSN i.e. a number of different Passive attacks, Denial of Service attacks, physical attacks, false node attack, etc.

By going through the related work it became pretty obvious that our work is different from other works. The work discussed above have either proposed an IDS scheme for a single security attack on WSN or they have just done a survey. in a way that we have not only focused on multiple attacks. But we have focused not only on multiple attacks with their in-depth study but also presented and IDS for detection of multiple WSN security attacks.

IV. Attacks on S-MAC

There are several kinds of common network attacks on S-MAC such as a Collision Attack, Unfairness Attack, Exhaustion Attack, Sinkhole Attack and Wormhole Attack [15]. We have briefly discussed all of the attacks with their detection methods and detection mechanisms. Below are the brief descriptions of network attacks on S-MAC:

- Collision Attack
- Unfairness Attack
- Exhaustion Attack
- Sinkhole Attack
- Wormhole Attack

A. Collision Attack

This attack occurs when legitimate nodes tend to communicate with each other, and the rival nodes start sending

data packets in these overlapping periods in order to hinder legitimate communication. In this way, the packet sent by the legitimate node gets lost, and the node has no other choice but to wait to find or acquire another medium for transmitting the RTS/ CTS packet. In order for a node to retransmit, it spends its energy over and over again for the very same packet, and this consumption eventually results in the reduction of energy. Normally, one byte is enough for making a CRC error in addition to disabling the data packet [16].

Advantages

- Power is consumed periodically in each data packet and is difficult to detect.
- This attack also culminates the ACK packet which results in exp. backoff message and wastes the battery.
- It can be launched anywhere in the entire network, and the attacker does not have extra capabilities.
- It weakens data integration in the MAC layer.

Detection Method

- Misbehaviour detection techniques

Defensive Mechanism

- All countermeasures of congestion attacks

B. Unfairness Attack

In S-MAC procedures, control is entirely employed by each node. All nodes transmit RTS packets so that they can request to attain the medium in which a CTS packet is sent back to the demanded, desired node. The medium is competed for in a particular node in each time vacancy. The first node tends to attain the medium, but the illicit nodes also get the benefit of this method and transmit the data packet with a low waiting time duration. It repeatedly transmits such packets to attain the medium and, hence, causes a hindrance for the legitimate nodes to have maximum access to the medium [16].

Attack effects

- Decrease in the services of effective networks.
- Nodes are desperate to have access to the medium.
- Limited access of nodes to the medium and can paralyze the usual communication within the medium.

Detection Methods

- Misbehaviour detection techniques

Defensive Mechanism

- Employment of smaller frames

C. Exhaustion Attack

The legitimate and rival nodes are installed in WSN in an open milieu. S-MAC procedures deal with the CTS/RTS method and are known for their capacity of transmission. Therefore, while attaining the medium, a node should transmit an RTS data packet and, in return, the receiver should send a CTS data packet [17]. The rival nodes [18] usually take advantage of this method, and the demanded node constantly transmits CTS data packets, as a result of which the network gets weakened or gets overloaded with the amalgamation of both legitimate and illegitimate nodes, further resulting in an exhaustion attack.

D. Sinkhole Attack

In such attacks, the rival nodes (or the compromised nodes) exhibit their attractiveness to the nodes to illustrate all of their traffic data from their constituency. Therefore, all the data packets' transfer is intended for the base station which in turn is drawn by the rival nodes. In order to have full autonomy over the data transfer [28], the compromised node aims for its adjacent nodes. The sinkhole attack [10] is started by the rival nodes from the adjacent nodes that are very close to the base station.

E. Wormhole Attack

In a wormhole attack, a link is developed by the illegitimate/ compromised node between two specified points in the network and this link is known as the wormhole link. This kind of directness of the wormhole link can only be made with the help of wireless transmission, optical fibre or wireline. The moment this type of direct connection (wormhole link) [5] is developed, the communication is captured by the rival nodes, and they channel the nodes from the origin to the other endpoint, known as the destination point.

Attack Effects

- False routing information.
- Alteration in the network topology.
- Packets alteration by wormhole nodes.
- Alteration in the normal flow of messages [28].

V. Methodology

In this section, we are going to discuss the analysis of Collision and Exhaustion attacks on the Wireless Sensor Nodes. For that, we have used a simulation model to implement a secure MAC in MATLAB. For the simulation model, we have used the following vital parameters.

A. Simulation Model

Table I shows the parameters used for the simulation model along with their values:

TABLE I. Year Wise Treatment Frequencies

Parameters	Values
Sensing Area Dimensions (X * Y sq. m)	50 m x 50 m
Legal nodes	14
Intruder nodes	5
Sink node	1
Dimension of sink node (X * Y sq. m)	25 x 25m.
Transmission Energy	50μJ
Received Energy	30μJ
Idle Energy Consumed	5μJ
Data Rates	250kbits/s

B. WSN Deployment

Fig. 3 below shows the wireless sensor nodes' network deployment. There are 20 nodes in which 14 nodes are the transmitting nodes, and one is the sink node. The five (5) nodes are acting as intruders. We have deployed these nodes in the x and y plane. All the nodes are going to transmit the data to the sink node which is located in the x and y plane at the location of (25, 25) in meters. Different locations are given to the nodes. The nodes are deployed randomly.

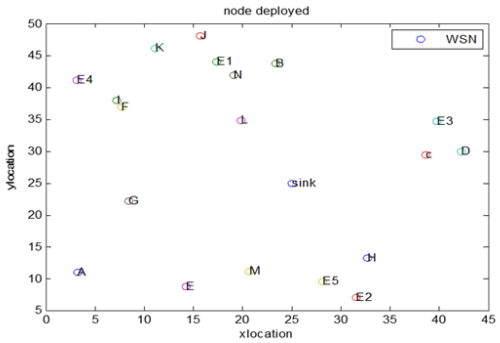

Fig. 3. Nodes deployed in our wireless network

C. Key Features of our Defensive Mechanism

Efficient Network Energy Utilization - Our exhaustion attack on the MAC layer node repeatedly sends RTS and CTS packets, due to which energy is consumed each time by sending these control packets again and again. Our defensive mechanism detects collision attacks which detect intruder nodes, and thus we can save network energy in this way.

Network Quality - S-MAC collision attacks are continuously being introduced in a WSN environment which loses the data packets and hence decreases the successful data packet transmission rate, which in turn affects network quality. Our defensive mechanism detects collision attacks efficiently. Decreasing the collision ratio in each node can improve network quality.

D. Intrusion Detection Mechanism

We chose the following statistics as intrusion indicators in the intrusion detection part:

Collision Ratio (Rc) - It is defined as the detection of the collision time for a node per second.

Probability of data packets' successful Transmission (PST) - A successful transmission can be defined as the sending and receiving of a packet by a node correctly. The probability of data packets' successful transmission is the ratio between the successful transmissions to the total number of data packets transmitted.

RTS packet arrival ratio (RRTS) – Defined as the number of RTS packets successfully received by a node per second. We collected the values of all indicators and estimated the intrusion probability. According to these values, we can conclude whether there is an intruder or not. For this we use the soft function which is given below:

$$y(x) = \frac{1}{1 + \exp\left[-A \times (x - C)\right]} \tag{1}$$

In Equation 1, A is the slope parameter. If the value of A is bigger, the slope is steeper, and C is the centre of the curve. From this equation, we can calculate the probabilities of the above-discussed intruder.

We generated the random values for collision, data packets' successful transmission and the RTS data packet arrival ratio (RRTS). We put the values of all these intruders in the above equation and found out the probability for each of them. The following are the results we achieved after putting random values in the above formula:

1) By inputting the values of the collision ratio in the soft function, we get the probability of collision, which is called PC.
2) By inputting the values of data packets' successful transmission ratio, we get the probability of the total, which is called PT.
3) By inputting the values of RTS data packets' arrival ratio, we get the probability of exhaustion, which is called Pe.

The shape of the curve can be adjusted by changing the A and C parameters. We can find the next values of $A(k)$ and $C(k)$ from the equations below:

$$A\left(k+1\right) = A\left(k\right) + \alpha \times \frac{\partial J}{\partial A} \tag{2}$$

Where $A(k)$ is the initial condition value; α is a value between 0 and 1.

$\frac{\partial J}{\partial A}$ is given us:

$$\frac{\partial J}{\partial A} = 2\left(yd - y\right) A\left(k\right) / \left(1 + \exp^{A(k)*(x - C(k))}\right)^2 \tag{3}$$

Where the actual value is y and the desired value is yd.

$$C\left(k+1\right) = C\left(k\right) + \alpha \times \frac{dJ}{dC} \tag{4}$$

Where $C(k)$ is the initial condition value; α is a constant value between 0 and 1.

$$\frac{dJ}{dC} = 2\left(yd - y\right) \frac{-A\left(k\right) \exp\left(-A\left(k\right) \times \left[x - C\left(k\right)\right]\right)}{\left(1 + \exp(-A(k) \times \left[x - C\left(k\right)\right])\right)^2} \tag{5}$$

In Equation 5, the actual value is y, and the desired value is yd.

E. Criteria for Attack Detections

Criteria for detection of Exhaustion Attack: Fig. 4 shows the criteria for the exhaustion attack. We got the value of exhaustion from the soft function by inputting the values of the RTS data packets' arrival ratio. The probability of success is added to the probability of exhaustion and compared with the threshold. The threshold is set, and then this summation

result is compared with the threshold. If the sum is greater than the threshold, then the attack is found. Otherwise, there was no attack. We set the threshold higher than the probability of success for our results.

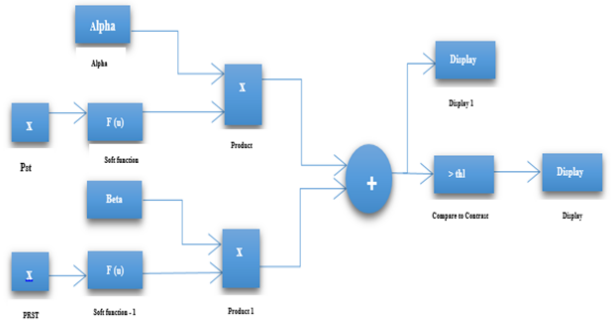

Fig. 4. Criteria for detection of Exhaustion Attack

Criteria for detection of Collision Attack:: Fig. 5 shows the criteria for the detection of a collision. In this figure, it is clear that when we got the probability of success from the soft function, then it is scaled by phi (ϕ). Similarly, we got the probability of collision from the soft function by inputting the values of the collision ratio, then scaled by theta (θ). The probability of success is summed individually with the probability of collision. As the above process shows, the probability of success is added to the probability of collision and then compared with the threshold, thus attaining a result. The threshold is set, and then this summation result is compared with the threshold. If the sum is greater than the threshold, then there was an attack. Otherwise, no attack occurred. We set the threshold higher than the probability of success for our results.

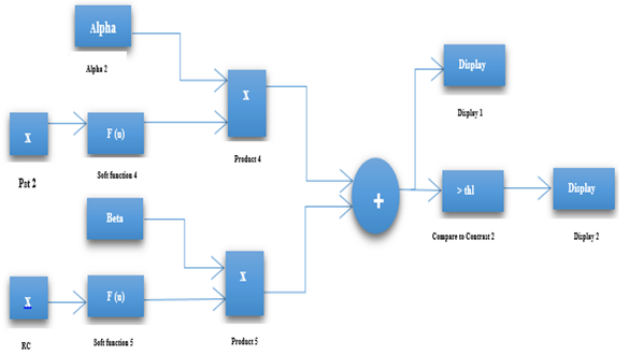

Fig. 5. Criteria for detection of Exhaustion Attack

VI. Experiment Results and Analysis

A. When No Collision Attacks were Found

Fig. 6 shows the graph as it appears when the values of E and F are changing. The next values of E(N) and F(N) are defined above. The graphs are:

- The square graph (green) is the graph of the probability of collision.
- The circle (blue) graph shows the probability of success.
- The dashed graph shows the threshold.
- The (red) solid line graph shows the sum of probability of success after multiplying with phi (ϕ) and the probability of collision after multiplying with theta (θ).

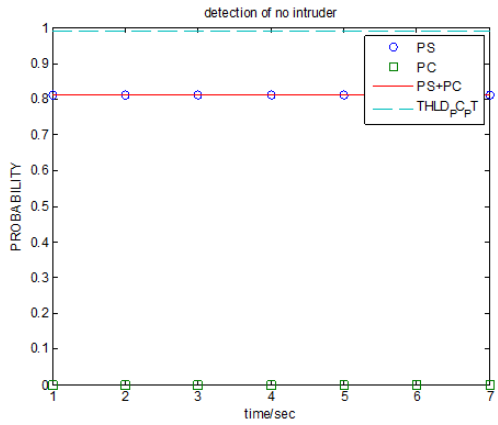

Fig. 6. No Collisions Found

B. When Collisions are Found

In Fig. 7, the (sum) solid line graph is greater than that of the threshold dashed graph, which means there is an intruder in the network.

C. Comparison of Delay to show Collision Attack

Fig. 8 shows the behaviour of nodal PS+PE transmission when there is no intruder and when there is an intruder. The delay of nodes is not high when there is no intruder. As the solid graph (blue) shows, it is clear that the delay of nodes transmitting without an intruder in the network is less than that of the delay when there is an intruder in the network. The solid (blue) graph describes the delay of nodes when there is no intruder in the network. When there is an intruder in the network, then the delay rises abruptly and increasing

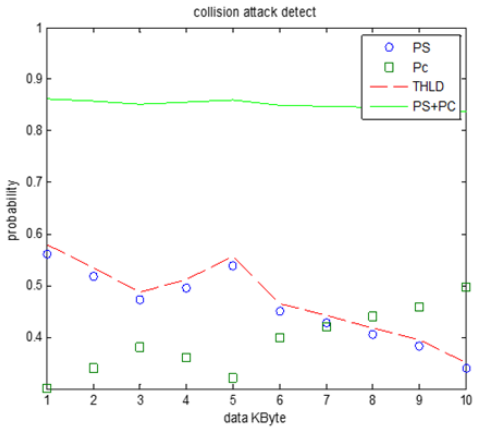

Fig. 7. Collisions Found

as compared to that of delays of nodes when no intruder is present. This unexpected increase in the delay shows that a collision occurred while transmitting the data. Therefore, the delay increased because of the retransmission of the packet. The (green) dashed graph shows the delay when there is an intruder in the network. This abrupt change in the graph is indicative of an intruder. When collisions occur, the node will retransmit the packet, and in this way, the delay is increased.

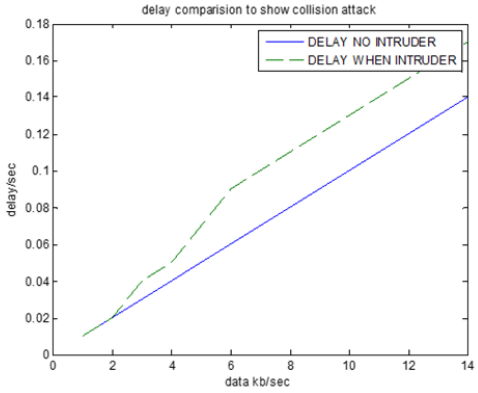

Fig. 8. Behaviour of nodes

D. When no Exhaustion Attacks are found

Fig. 9 shows a comparison of the probability of success with the probability of exhaustion. This graph is also a multigraph in which:

- The square graph (green) shows the probability of exhaustion.
- The circle graph (blue) shows the probability of success.
- The dashed graph shows the threshold.
- The solid (red) one is the sum graph of the probability of success and probability of exhaustion.

We completed a comparison of the sum graph with the threshold graph. If the sum graph is greater than that of the dashed graph (threshold), then it means there is an intruder in the network. So, here there is no intruder.

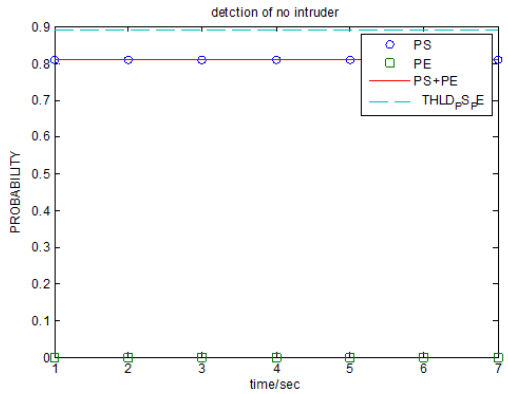

Fig. 9. No Exhaustion Attacks Found

E. When Exhaustion Attacks are found

Fig. 10 clearly shows that there is an intruder since the sum solid line graph (red) is greater than that of the dashed graph which represents the threshold.

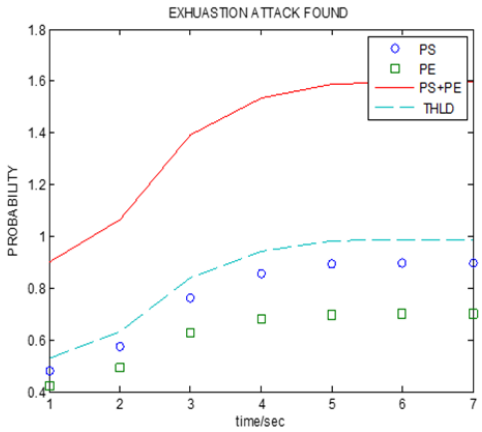

Fig. 10. Exhaustion Attack Found

F. When Exhaustion Attack is Detected

Fig. 11 clearly shows that the exhaustion attack is detected.

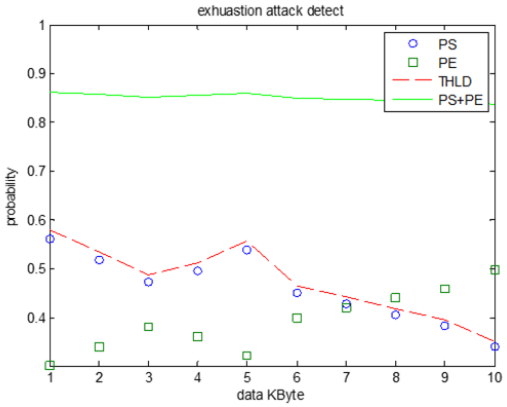

Fig. 11. Exhaustion Attack Detected

G. Exhaustion Attack

The graph in Fig. 12 shows the behavior of sensory nodes before and after detection of an exhaustion attack.

- The circle graph (blue) shows the exhaustion attack (repeated RTS packet arrival) and the waste of energy in (response of CTS) the presence of the intruder.
- The square graph shows energy dissipation after the detection of the intruder.

VII. Discussion

Our work has targeted the WSN which on one side is a promising communication network and provides the user a number of benefits like lower cost, lower power consumption, and easy deployment [26] and also supports a number of important real-life applications. While on the other side, Security

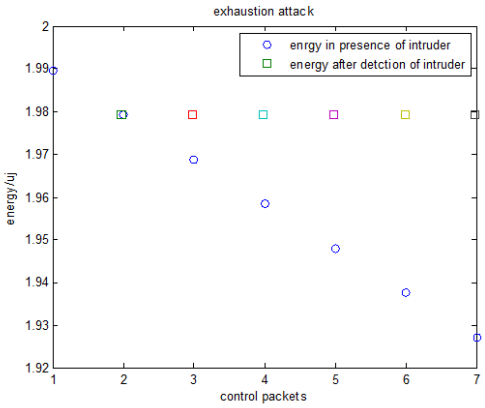

Fig. 12. Behaviour of Nodes

is also becoming a concerning issue for the WSNs because mostly the networks' nodes are deployed in some antagonistic area where the nodes have small memory, limited amount of energy [27] and this results in occurrence of a number of security attacks which sometimes jam the legitimate network traffic and can also leak sensitive information.

Security being a sensitive issue for WSN and the security attack targeting the network layer resulting in disturbed communication in important real life environment like military, we chose to analyze the Intruder attacks like Unfairness attack, Exhaustion attack, Sinkhole attack and Wormhole attack on S-MAC in a sensor network. We have presented an Intrusion detection system (IDS) to detect the attacks and an Intrusion Prevention System (IPS) to prevent those attacks in future. But this is done at smaller level to first check whether it will give us the expected results or not. Our simulation results showed the results as expected. This proved the effectiveness of our soft IDS and IPS mechanisms. We might continue this work to make it able to be implemented in some real- time environment for the detection of Intruder attacks to make it more fruitful.

VIII. Conclusion

In this research, we have focused on securing a Wireless Sensor Network against collision and exhaustion attacks. As in MAC protocol of WSN, the intruder can disturb the performance of the whole WSN by just depleting the battery source of legitimate nodes. We have adopted an Intrusion detection mechanism for the detection of different kinds of intruders' attacks. Then we developed a soft decision mechanism to detect intrusions and exhaustion attacks in WSN. A preventative mechanism has also been developed which helps the node to avoid such intruder attacks. The simulation results have proved the effectiveness of our mechanism by showing how a lifetime of a node has increased along with the network performance with reduced energy consumption, reduced delay on the node and successful transmission. In the future, we will be focusing on other emerging attacks on the MAC layer as well as S-MAC. In the future, we plan to extend our implemented detection mechanism to defend against other emerging attacks like DoS attack on WSN. This extension can lead to its implementation in different real-life scenarios like battlefields, health departments and also for other critical missions that need a cutting edge method for secure data transmission.

References

[1] F. Dong., J. Yang., C. Xiong., H. Ding, and Y. Zhang, "Research and implementation of a hybrid mac protocol for wireless sensor networks based on clustering structure," *Int J Recent Sci Res.*, vol. 9, no. 10, pp. 29 131–29 134, 2018.

[2] F. Z. Djiroun and D. Djenouri, "Mac protocols with wake-up radio for wireless sensor networks: A review," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 587–618, 2016.

[3] K. A. Memon, M. A. Memon, M. M. Shaikh, B. Das, K. M. Zuhaib, I. A. Koondhar, and N. U. A. Memon, "Optimal transmit power for channel access based wsn mac protocols," *INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND NETWORK SECURITY*, vol. 18, no. 7, pp. 51–60, 2018.

[4] R. Ramya, G. Saravanakumar, and S. Ravi, "Mac protocols for wireless sensor networks," *Indian Journal of Science and Technology*, vol. 8, no. 34, p. 1, 2015.

[5] D. Mohammed, M. Omar, and V. Nguyen, "Wireless sensor network security: Approaches to detecting and avoiding wormhole attacks," *Journal of Research in Business, Economics and Management*, vol. 10, no. 2, pp. 1860–1864, 2018. [Online]. Available: http://scitecresearch.com/journals/index.php/jrbem/article/view/1413

[6] V. Casola, A. De Benedictis, A. Drago, and N. Mazzocca, "Analysis and comparison of security protocols in wireless sensor networks," in *2011 IEEE 30th Symposium on Reliable Distributed Systems Workshops*. IEEE, 2011, pp. 52–56.

[7] K. Chelli, "Security issues in wireless sensor networks: Attacks and countermeasures," in *Proceedings of the World Congress on Engineering*, vol. 1, no. 20, 2015.

[8] A. Rai, S. Deswal, and P. Singh, "Mac protocols in wireless sensor network: a survey," *International Journal of New Innovations in Engineering and Technology*, vol. 5, no. 1, pp. 95–101, 2016.

[9] Y. Rao, Y.-m. Cao, C. Deng, Z.-h. Jiang, J. Zhu, L.-y. Fu, and R.-c. Wang, "Performance analysis and simulation verification of s-mac for wireless sensor networks," *Computers & Electrical Engineering*, vol. 56, pp. 468–484, 2016.

[10] M. Sharma, A. Tandon, S. Narayan, and B. Bhushan, "Classification and analysis of security attacks in wsns and ieee 802.15. 4 standards: A survey," in *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall)*. IEEE, 2017, pp. 1–5.

[11] S. Kaur and S. Sharma, "A review on various routing protocols based on clustering in wsn." *International Journal of Advanced Research in Computer Science*, vol. 8, no. 7, 2017.

[12] W.-M. Song, Y.-M. Liu, and S.-E. Zhang, "Research on smac protocol for wsn," in *2008 4th International Conference on Wireless Communications, Networking and Mobile Computing*. IEEE, 2008, pp. 1–4.

[13] G. Gautam and B. Sen, "Performance analysis of 802.11 and smac protocol under sleep deprivation torture attack in wireless sensor networks," *International Journal of Computer Sciences and Engineering*, vol. 3, no. 5, pp. 317–322, 2015.

[14] S. Otoum, M. Ahmed, and H. T. Mouftah, "Sensor medium access control (smac)-based epilepsy patients monitoring system," in *2015 IEEE 28th Canadian conference on electrical and computer engineering (CCECE)*. IEEE, 2015, pp. 1109–1114.

[15] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *IEEE Communications surveys & tutorials*, vol. 13, no. 2, pp. 245–257, 2011.

[16] P. Sinha, V. Jha, A. K. Rai, and B. Bhushan, "Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of osi reference model: A survey," in *2017 International Conference on Signal Processing and Communication (ICSPC)*. IEEE, 2017, pp. 288–293.

[17] T. Borgohain, U. Kumar, and S. Sanyal, "Survey of security and privacy issues of internet of things," *arXiv preprint arXiv:1501.02211*, 2015.

[18] M. Tiloca, D. De Guglielmo, G. Dini, G. Anastasi, and S. K. Das, "Jammy: A distributed and dynamic solution to selective jamming attack in tdma wsns," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 4, pp. 392–405, 2017.

[19] M. Pawar and J. Agarwal, "A literature survey on security issues of wsn and different types of attacks in network," *Indian J. Comput. Sci. Eng*, vol. 8, pp. 80–83, 2017.

[20] Osanaiye, Opeyemi and Alfa, Attahiru and Hancke, Gerhard, "A statistical approach to detect jamming attacks in wireless sensor networks," *Sensors, Multidisciplinary Digital Publishing Institute*, vol. 18, pp. 1691, 2018.

[21] V. Mittal, S. Gupta, and T. Choudhury, "Comparative Analysis of Authentication and Access Control Protocols Against Malicious Attacks in Wireless Sensor Networks," pp. 255–262.

[22] I. Butun, S. D. Morgera, and R. Sankar, "Wireless Sensor Networks," vol. 16, no. 1, pp. 266–282, 2014.

[23] I. Krontiris, T. Dimitriou, and T. Giannetsos, "Intrusion Detection of Sinkhole Attacks," pp. 150–161, 2008.

[24] Chen, Honglong and Lou, Wei and Wang, Zhi and Wu, Junfeng and Wang, Zhibo and Xia, Aihua, "Securing DV-Hop localization against wormhole attacks in wireless sensor networks",*Elsevier, Pervasive and Mobile Computing*, pp. 22–35, vol. 16, 2015.

[25] K. S. Selvam and S. P. Rajagopalan, "Security Analysis with respect to Wireless Sensor Network – Review," vol. 6, no. 4, 2017.

[26] Sharma, Kalpana and Ghose, MK and others, "Wireless sensor networks: An overview on its security threats", *IJCA, Special Issue on "Mobile Ad-hoc Networks" MANETs* , pp. 42–45, 2010.

[27] Dinker, Aarti Gautam and Sharma, Vidushi, "Attacks and challenges in wireless sensor networks", *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 3069–3074, 2016.

[28] M. Pawar and J. Agarwal, "A literature survey on security issues of wsn and different types of attacks in network," *Indian J. Comput. Sci. Eng*, vol. 8, pp. 80–83, 2017.

[29] Can, Okan and Sahingoz, Ozgur Koraytitle, "A survey of intrusion detection systems in wireless sensor networks", *IIEEE, 2015 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO)*, pp.1–6, 2015.

[30] Shahzad, Furrakh and Pasha, Maruf and Ahmad, Arslan, "A survey of active attacks on wireless sensor networks and their countermeasures",*arXiv preprint arXiv:1702.07136*,2017.