Security Techniques Against Power Exhausting Attacks in WSN: A Fundamental Study

Jaya Kaushik a, Dr. Naresh Grover[b]

[a]Department of ECE. Manav Rachna International University, Faridabad, Haryana
[b]Dean Academics, Manav Rachna International University, Faridabad, Haryana
Email: lsntl@ccu.edu.tw

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract: DoS attack is being considered for the wireless sensor network, where the attack affects the battery life of the devices connected in the network. The basic goal of the DoS attack is just to reduce the availability of the necessary devices connected by reducing the battery lifetime. The connected devices are kept on unnecessary use which results in the reduction of the battery life and effects the battery management. In the proposed work, a novel methodology shall be taken for the better management of the battery lifetime of the devices connected. In case if any of the connected devices detects low power or when not in use, it goes to sleep mode for the better usage of the battery power. In the discussed methodology the system is made prone to such type of attacks and also works for the detection of such types of attacks and nodes too. In the work presented the major consideration is for the explanation and in-depth knowledge about the domain and specially for the energy exhausting attacks and techniques. On the basis of the survey considered a specific problem is being considered in the work for which a tentative solution is also provided with the points that are to be considered for the evaluation of the work. In the proposed methodology RSSI value along with information of the route is being used for the discernment of the malicious nodes and for ensuring the security of the network, the cluster mechanism is being considered for the better and improved results. The enhancement in the previous work is being done for the better power management.

Keywords: WSN DoS Energy Exhausting Attacks RSSI Fifth keyword

1. Introduction

Wireless Sensor Networks may be described as self-configured networks and less without wire networking networks that track physical or environmental circumstances including temperature, son, pressure, vibration, movement or pollution and that collectively send the information via the network to a major position or sink, place the data might monitored and evaluated. A sink or base station serves as a user-to-network interface. Through making queries and acquiring data through sink you may get the correct knowledge from the network. In general, a network of without wire sensors is having huge number of sensor nodes. The sensor nodes may communicate via one another via radio signals. A without wire sensor node includes sensor and computing resources, radio transceivers and control device. instinctive, the single nodes within a WSN are support limited: which are having constrained processing speed, efficiency for data storing and bandwidth of communication. When the sensor nodes are placed, they also have to self-organize an effective network framework for multi-hop communication. While the onboard sensors begin to collect useful information. Wireless sensor systems often respond to requests from a "control site" for guidance or sensing samples. Both continuous or event guided mode of the sensor nodes might use. The Global positioning system or the Local positioning system might consider for the detection of the location. Wireless sensor devices can be fitted with "acting" actuators in some conditions. Such networks are often referred to more precisely, as defined in (Akkaya et al. 2005) [1], as without wire sensor and actuator networks.

(WSN) allow new implementations and need, because of a variety of constraints, non -traditional protocol construction paradigms. Thanks for need for less system complexity and less power usage (i.e. high network life), a reasonable balance must be sought within connectivity and signal/data analysis capacities. It has been a subject of significant initiative over the last decade in the area of research, the standardization phase and technological innovation (Chiara et. al. 2009)[2]. Currently much of WSN analysis focuses on the structure of energy-efficient and numerical techniques and protocols, the implementation scope is limited to purely data-oriented tracking and reporting applications (Labrador et al. 2009) [3]. A Cable Mode Transition algorithm (CMT) is proposed through the authors in (Chen et al. 2011) [4] which specifies both the K extension of a terrain and the K-connectivity of the network as the minimum number of active sensors. Specifically, it determines cable sensor inactivity intervals without impacting network range and connection criteria based solely on local information. Author in [5] have presented the network framework for the data gathering in WSN environment. The major goal of the work presented was to avoid the delays while the data collection in WSN. In (Matin et al. 2011) [6], the researchers took into account the spatial network deficits relay nodes and used algorithms based on (PSO) particle swarm optimization to place optimum sink location in relation to such some nodes in order to address the difficulty of lifetime. In addition, energy-efficient transmission was discussed (Paul et al., 2011[7]; Fabbri et al. 2009[8]). The authors proposed a geometric solution in (Paul et al. , 2011) to find the optimal sink location to maximize network

life. Wireless sensor network work has found homogeneous sensor nodes mostly on the time. Yet researchers now focus on heterogeneous sensor networks, in which the sensor nodes differ in their capacity.

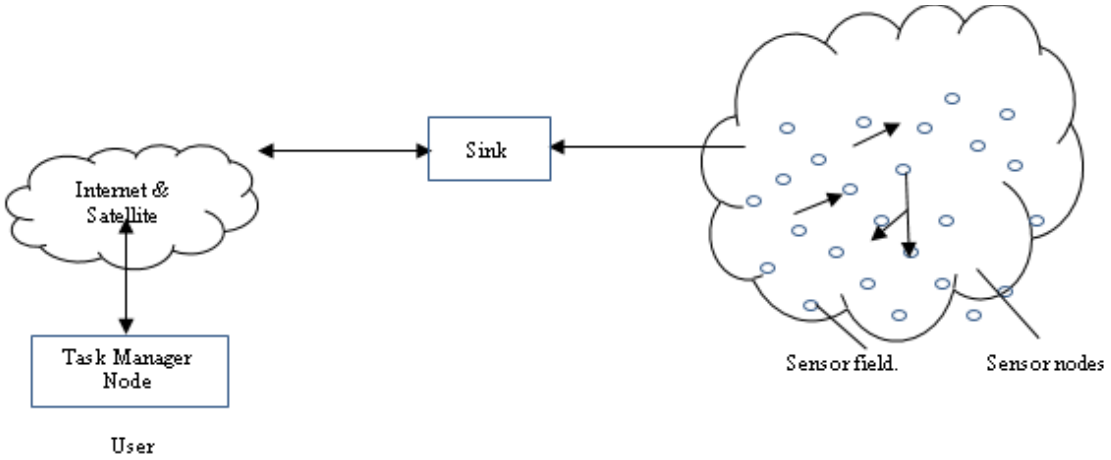

Figure 1. A typical Wireless Sensor Network.

1.1. Characteristics of WSN

a. In WSN, every single node behaves like a node and also like router too.
b. Multi-hop radio relaying- In the case when the sender of the message and receiver of the same are out of the network then the WSN is termed as the multi-hop network,
c. WSN has dynamic topology.
d. WSN can easily be deployed.
e. WSN is distributed in nature.
f. Nodal connectivity is intermittent.
g. The sensor nodes implemented in the network are attached with some features like less power consuming.
h. Large number of users can be connected to the single node and also the user mobility of the nodes is quite higher.
i. It has Mobile and dynamic nature and requires least human involvement to organize the structure.
j. WSN is robust due to decentralized administration.
k. WSNs are scalable any number of nodes can connect the network.
l. Network facilitates the nodes addition and deletion at moment of time.
m. Static infrastructure is not required in the case of the wireless network.

1.2. Applications of WSN

Because of the pliability in evaluating difficulties in diverse usage fields, WSNs became very popular and are having the ability to alter the individuals living in varied domain areas. A wide variety of applications has been successfully implemented [9][10][11][12][13][14].

- **Military applications:** without wire sensor networks are expected to be a vital segment for the army operations, management, communication, computer systems, surveillance, frontline tracking, detection and pursuing frameworks.

- **Area monitoring:** In the field monitoring area, the sensor nodes are located in a location that tracks a certain phenomena. When sensors find the event (pressure, heat etc.) being controlled, the incident is recorded to the defined base stations, where the action is taken.

- **Transportation:** WSNs are gathering actual traffic information for later feeder models to caveat drivers for crowd and traffic issues.

- **Health applications:** Health applications for the sensor networks include promoting disabled devices, automated patient monitoring, diagnosis and pharmacy administration in clinics, telemonitoring of human physiological data and tracking and monitoring physicians or patients in hospitals.

- **Environmental sensing:** The word Environmental Sensor Network has been considered to facilitate a large range of WSN applications for global science research. It covers volcanoes, trees, glaciers, lakes, etc. Certain crucial applications are mentioned as under:

  - Monitoring of pollution in Air,

- Detection of fire in Forest,
- Management of Greenhouse,
- Detection of Landslide.

- **Structural monitoring:** without wire sensors are well used for monitor traffic in construction and frameworks, like as bridges, flyovers, dike, tunnels etc., allowing engineering operations to distantly control properties having expensive site visits.

- **Industrial monitoring:** For machinery (CBM) condition-based maintenance, without wire sensor networks are well built to be a significant cost cutting and permits various functionalities. As of wired methods, cost of wiring also makes hard for the deployment of sensors specifically required for the application.

- **Agricultural sector:** The farmers are free from cable management in a difficult environment through a wireless network. Via automated irrigation system the crucial resources like water can be efficiently considered and also the waste of the same can be reduced.

1.3. Security Goals in WSN

Special safety approaches are required for sensor networks with less computational resources, storage, bandwidth and resources. The hardware and power limitations of the sensors make it difficult, in terms of availability, Integrity, authentication, freshness, confidentiality, access control and desertion, to fulfil the security needs of ad hoc networks [15].

- **Availability:** The availability provides reactivity and response time protection to send single source information to the correct user. The process also depicts that network processes are present if necessary, for legitimate parties and ensure network services despite denial of service attack (DoS).
- **Integrity:** It is a service that assures as while communication the information is not changed. Integrity secures the network from communications being inserted or changed.
- **Confidentiality:** guarantee the node information is not available or revealed only to the receiver of the node.
- **Freshness:** WSNs makes available few metrics of time; to ensure that every packet is new. The refreshness of the packet means that the packet is fresh and also no malicious node replays the previous packets.
- **Authentication:** The malicious node is not only confined to changing the data packet. He can also add more packets. The user will then verify that the used data comes from the right source. In addition, authentication is necessary for several activities by constructing WSNs.
- **Access control:** Provides the legal participants with a way to detect communications from external network channels.
- **Non-repudiation:** Ensures that the message source cannot doubt that the message was sent [15].

1.4. Attacks in WSN

The literature records a number of attacks on WSNs. Various measurements were suggested to address such attacks. The key types of attacks are listed below, and also the attacks can be further explored on the basis of the layers specification.

A definition of malicious activities is to provide a differentiation within passive and active kinds of attacks.

The passive type of attacks are like restricted, attacks in traffic monitoring and review. Such attacks are easier to carry out (the right receiver is enough) and hard to notify. As the malicious user makes no change in the information exchanged. The attacker's purpose can be to learn confidential information or to know the main nodes in the network (cluster - head), to examine routing data to made an active type of attack.

A malicious user attempts to delete or alter packet received on the network after successful attacks. It is also able to inject new packets or even can reforward the previous packets just to disrupt network processing or to make a condition of a service denial. The major well-known active types of attacks are as under:

- **Tampering:** is a product of the attacker's physical entry to the sensor node, which helps to receive again cryptographic material like as keys considered for ciphering [16].
- **Black hole:** A sensor node invert routing data to compel the packet to pass through it; the primary duty, then, is to relay nothing, producing a sink or black hole in a network [17].
- **Selective forwarding:** As mentioned at an end above, a node plays a router function. Attacker nodes can spurn to forward and can drop those packets in the case of the selective sending attack.

- **Sybil attack:** Author in [18] defined this malicious activity as "a malicious system that illegitimately takes multiple identities," an attacker may be the part of the distributed technique like voting using the identities of the other nodes.
- **HELLO flood attack:** many routing protocols consider the "HELLO" packets to identify next nodes in the network and therefore to define network topology. The simplest malicious activity on an attacker is to deliver an inundation of this messages to the network and to block the transmission of other messages.
- **Jamming:** A well-known without wire communication attack involves dislocating the radio channel by transmitting worthless frequency band information. This intermittent, temporary or permanent jamming will occur [19].
- **Blackmail attack:** A attacker declares that the other legitimate sensor node is an attacker in order to remove it from the communication. In the case when the attacker succeeds to counter a notable number of sensor nodes, then is able to create disturbance in the communication process.
- **Exhaustion:** The goal is to exhaust the complete energy sources of the legitimate sensor node, via forcing it either to compute or to excessively collect or send packet [20].
- **Wormhole attack:** Malicious users are strategically located at many types ends of the network here. They will get packets and repeat the same through a tube in various segments [21].
- **Identity replication attack:** The hacker may also create duplicates of the sensor nodes to catch the majority of traffic in information and place them in different parts of the network. Like the Sybil attack, the identity replication attack [22] is relied on various physical nodes sharing the same identity. This attack can be mounted as it is not known in a WSN that a wireless sensor node is affected.

1.5. Issues in WSN

The architecture of sensor networks is a collection of the challenges seen in wireless ad - hoc frameworks. Wireless, fault lines without links communicate with sensor nodes. The major issue with the nodes is the non-chargeable battery. The techniques should be designed by keeping the issue of power consumption into consideration, so that the life time of the sensor nodes might maximize. Akkaya et al., 2005 have properly justified the issues related to the WSN and also the issues after simulation of the network on various platforms is also discussed ([25], SensorSim, Tossiim). Let us now address in more depth the individual structure issues.

- **Fault Tolerance:** The sensor nodes are quite pregnable are always considered over the region where the environment is human friendly which creates the problem of the battery replacement. The issues for replacement of nodes because of the hardware failure, power failure, etc is rosed. In the case of the WSN the nodes failure rate is quite high as compared to the wired system framework. The protocols are supposed to be efficient enough to explore the failure of the nodes as soon as possible to avoid the data losses and other major impacts over the network efficiency. This is particularly important for the design of the routing protocol that must make sure alternative paths are available for packet reprocessing. Various deployment systems have various criteria for fault tolerance.
- **Scalability:** Networks of sensors range from several nodes to hundreds of thousands. However, the intensity of installation is also vital. The density of the sensor nodes will be at the level when the node is having various neighboring nodes in its communication range for the processing of high - resolution information. The protocols considered for the sensor networks must be scalable to all such levels and manage sufficient performance.
- **Production Costs:** In almost all of the techniques for nodes deployment the sensor nodes are considered as the disposable products, sensor networks are comparable only when every single sensor node is manufactured considering price with traditional approaches. Ideally, the final cost for a sensor node is supposed to be near about $1.
- **Hardware Constraints:** That sensor node must at least include a sensor unit, a processing unit, a communication unit and an energy unit. Options can also include various built - in sensors or extra devices for location-conscious routing, such as a localization system. Nonetheless, that additional feature provides additional costs and increases the node's energy consumption and physical size. As a result, additional capabilities must always be weighed for price and less power needs.
- **Sensor Network Topology:** In spite of the fact that the WSN has enhanced in various ways, it is often electricity, power processing, memory and limited - resource communications networks. The consumption of energy is important among these restrictions and can be seen in the numerous algorithms, technologies and protocols aimed at saving resources and thus time augmentation the life of the network. Topology optimization is among main issues for reducing power usage in without wire sensor networks.
- **Transmission Media:** The transmission within the sensor nodes is usually carried out via radio communication through common ISM bands. But certain sensor networks consider optical or infrarot transmission, which benefits from the ability to be robust and virtually free of interference.

- **Power Consumption:** Various issues of the WSN are about the energy conservation and energy management in the network, as we have already seen. The size of the node decides the size of the battery. The software and hardware architecture must take careful note of the problems of energy efficiency. For example, data compression can degrade the power consumption in radio transmission, but it requires extra power for measurement and/or filtering. The power management also relies on the application; it may be appropriate in some implementations to shut off a sun-group of nodes to preserve power, whereas many applications needs all nodes to work together.

2. Energy For Security

Quantum lifetime node is usually restricted to the life span of a small battery, so that power is the critical resource cap. The extra energy used by sensor nodes because of security depends on:

- measurement required for security functions, such as ciphering, deciphering or signature authentication.
- Energy needed for protection material transmission and management (keys, etc.).
- Energy required for key storage.
- The goal is to minimize energy consumption by optimizing safety performance.
- When planning security measures for WSNs, energy is an important factor to consider. Conservation of node capacity and prolongation of network functionality.

2.1. Energy Exhausting Attacks

In the section below the major attacks for power exhausting are considered as, selfish, denial of sleep and collision.

A. Collision attack

The collision of the data packets is the major cause for the power loss. The malicious nodes have the information about the MAC protocols and can insert some fake messages into the network which results in the packet collision. In the contention based MAC protocols are RTS/CTS and ack control messages are being considered to avoid the data collision. In the case when the server is malicious then it don't obeys the rules of the MAC protocols for the networking operations. The time to pass is somehow mentioned over the header of the RTS message and the same is being considered by the malicious nodes to send the malicious content over the network.

B. Denial of sleep

In this sleep-assault strategy renege, the adversary node tries to reduce the sensor nodes ' lifetime through WBANs by increasing the working time of the sensor nodes. The primary objective of sleep renege is to force the nodes in WBANs to stay either during the wake - up process or during the active period. Just because of the rejection of the MAC protocols the energy consumption is affected by resisting the nodes from sleep and making them active without requirement. In the case when the malicious node is having the information about the layered protocol then it tries to manage the network accordingly for the communication cycle like Sensor-MAC[26], Timeout-MAC[27] and Berkeley MAC[27], because of which the nodes life reduces. Raymond et al.[29] in their work have differentiated WBANs as denial of sleep attacks in three different models: unauthenticated broadcast attacks, smart replay attacks, and full supremacy attacks.

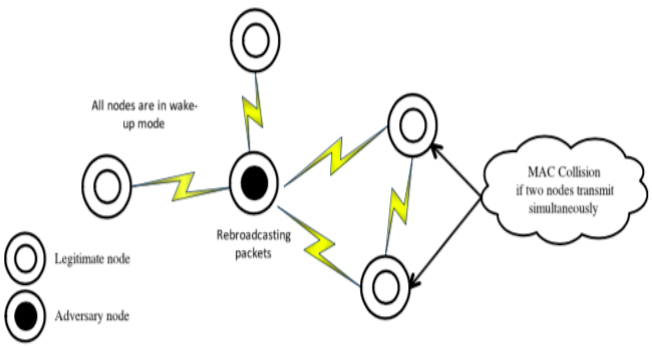

Figure 2. Scenario of a denial of sleep attack using broadcast packets.

C. Unauthenticated broadcast attack

The attacker node have the every information about the MAC protocol with this strategy attack while is not able to access the network. The competitor node transmits unauthenticated packets goes at the same time towards every of the nodes in the World Wide Web by emulating all the MAC protocol codes. Malicious data influence the sleep and listening phase of all WBAN nodes, which keeps the node transceiver in the audio period for messages. The malicious message or erroneous packet is deciphered and the source node data correlates. It is known as a system of mutual authentication[30].

To monitor or shake the process behaviour on the network, container-based MAC protocols (CTS)–(RTS), sync packets and (LPL) low power listening are considered. Thus, if the adversary node is constantly transmitting unauthenticated packets on the network for a longer duration, these packets are obtained and verified in the link layer of nodes as they assume that this packet are from their legitimate neighbouring nodes. Right after the authentication of the packets by nodes, this message will be discarded as fake packets.

D. Intelligent replay attack

In an intelligent play again attack the malicious node is fully aware of the MAC protocol while cannot enter the network. The malicious node will be considering its complete layer protocol knowledge to perform a smart play again attack on WBANs. SYNC packets are played again to save sleep for each node at the end of the duty cycle and to begin a new duty cycle. Hence, the nodes, such as Timeout-MAC (T-MAC)[27] and sensor-MAC (S-MAC)[26], are stored at wake - up and energy-free.

The sensor nodes considers the SYNC message to synchronize the active node cycle and sleep time sent at the beginning of each frame. Relying on the value of the SYNC message, the recipient node is recalculated to establish compatibility with the other nodes as soon as the SYNC messages are received. The malicious node notes the value of every node's sleep time, as shown in the SYNC message for retransmission of the SYNC message to all nodes[29]. In the case when SYNC packet is encrypted and the adverse node cannot interpret the sleep time, the node may still recognize the transition time from the sleep part of the frame to the SYNC period in the next frame by observing the action network.

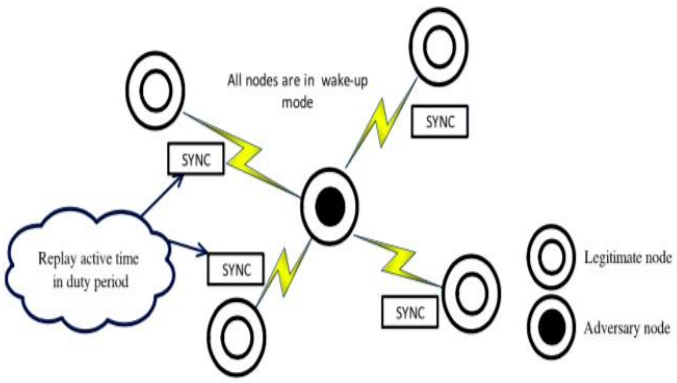

Figure 3. Scenario of a denial of sleep attack using an intelligent replay attack.

E. Full domination attack

Such kind of attack implies the opponent node have all about the MAC protocol and also may hit the network. It is among the major harmful kind of attacks on WANs. In almost all MAC protocols, such kind of attack raises energy usage by entering the network and gaining information about the layer protocols. A related intelligent replay attack is a total ascendancy attack against the Sensor-MAC (S-MAC) [26] or Timeout-MAC (T-MAC) [27] protocol. On the other hand, the malicious node don't revert the SYNC messages in this attack method. Rather, it changes the sleeping schedule of network nodes by fixing a new sleeping time for the sensor nodes (e.g., set the maximum value) for which the nodes cannot join sleeping hours. The time of sleep in the SYNC packets is when the nodes continue the cycle of sleep.

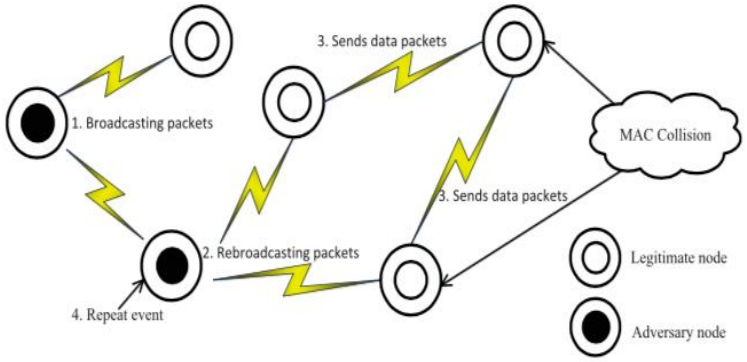

Figure 4. Scenario of a denial of sleep attack using full domination attack.

F. Selfish attack

In greedy attacks, the competing nodes use the MAC protocols to disproportionately considers the tools. MAC protocols depending on confrontation are more fragile than MAC Protocols dependent on the timetable. The MAC protocol on a calendar, like TDMA, allocates a predefined data transmission time slot to each node. The access point defines the assignment policy for time slots. Hence, it is quite hard for the malicious nodes to carry out an egoistic attack. The sensor nodes understanding the channel prior to sharing the messages in the schedule-based MAC protocol like CDMA / CA. In the case when the communication channel is free, the sensor nodes are waiting for the time interval of the DIFS before transmitting the messages. In the case when the transmission channel is active, the sensor nodes exponentially enhances the waiting time. While, the opposing nodes may always choose a shorter waiting time and have a better chance of accessing the web. The Valid nodes will wait longer and feel the channel which absorbs more electricity.

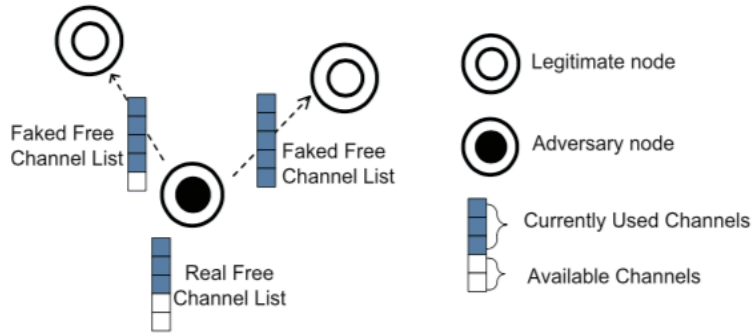

Figure 5. Scenario of selfish attack in multichannel WBNs.

Table 1. Summary of energy exhausting attacks in MAC protocols in WSNs.

EEM	**MAC**	**Unauthenticated broadcast attack**	**Intelligent replay attack**	**Full domination attack**	**Collision attack**	**Selfish attack**
C-BM	S-MAC	The sensor nodes are kept awaked by sharing fake messages over the time scheduled to listen	The nodes are kept awaked by resending the SYN packets while the time of synchronization	Modification sleep schedule to resist sensor nodes go to sleep during SYN packets	Collision or conflict by sharing unwanted CTS/RTS messages	Using short back off window
	T-MAC	Resisting nodes from sleep while the period of contention by the broadcast of	Replaying SYN to prevent nodes going sleep duration	Avoiding nodes from sleep by changing the	Causes collisions by sending fake packets	Using short back off window

		fake messages		SYN message		
	Wise-MAC	Resisting sensor nodes from sleeping by sharing fake data when the preamble data is received	Have fewer effect as compared to rest of the attack techniques	High energy loss when the nodes keep on looking the network to be active for participation	Access Collision by sharing fake messages	Using short back off window
	B-MAC	Just because of the PLP method the fake messages are received on regular interval	Less effect due to not using SYN packets	Just because the SYN message is not considered the effect is quite less	May perform collision attack if knowing duration information	Using short back off window
S-BM	Body MAC	The gateway node is affected more as compared to others	Just because of the SYN message it is quite hard to attack	hard to attack on sleep period of nodes	Sensor nodes are affected because of the data sharing while GTS slot time	Difficult to attack
	TDMA-based	Hard to attack because of predefined time slot	Hard to resend the SYN message while the sleep time	The nodes are less affected in sleep time	The nodes are compromised by sharing fake message during GTS slot time	Difficult to attack
	Med-MAC	As the time slot are adjustable for which the sleep time is less affected	Quite hard to compromise because of the consideration of beacon message for synchronizing	The sleep time of the nodes is less affected	Effect on access point and nodes in GTS slot time	Difficult to attack
H-BM	Z-MAC	As a specific time is assigned for each of the nodes because of which the affect is quite less	Quite hard to compromise in a low level of contention period	Less Effect on nodes in contention period	Effect on contention-free period in GTS slot time	Difficult to attack in contention period
	CA-MAC	Effect on nodes in low contention period	Just because of the beacon messages the affect is quite less	Less Effect on nodes in contention period	Less effect in contention period in GTS slot time	Difficult to attack
	G-MAC	While the period of collection the effect on gateway node is quite less period difficult in power saving mode	The GTIM or FRTS messages might be re-shared while collection period	Changing GTIM or FRTS messages to resist sleep	Less effect on nodes or access point	Effect on contention period

Table 2. Layer based attacks and possible security mechanisms in wireless sensor network.

Layer	Attacks	Security Techniques Defenses
Physical layer	Network Jamming	Priority messages, Lower duty cycle, Spread-spectrum techniques
	Tampering	Hiding, Tamper proofing
Data Link Layer	Collision	Error-correcting code
	Exhaustion	Rate Limitation
	Unfairness	Small Frames
Network Layer	Spoofed, altered or replayed routing information	Monitoring, Authentication
	Selective forwarding	Redundancy, Probing
	Sink Hole	Monitoring, Authentication, Redundancy
	Sybil	Authentication, Probing
	Worm holes	Authentication, Packet leashes by using geographic and temporal information
	Hello flood	Verify the bidirectional link, Authentication
	Acknowledgment Spoofing	Authentication
Transport layer	Flooding	Client puzzles
	Desynchronization	Authentication
Application Layer	Attacks on reliability and Clone attack: Clock skewing, Selective message forwarding, Data aggregation distortion	Unique pair wise keys and cryptographic approach. Authentication can be used to protect any data integrity Encryption is an effective approach for data confidentiality protection

2.2. Security Services

WSN's general safety objectives [31] are confidentiality, integrity, authentication, accessibility, survival, efficiency, freshness and scalability as outlined in Table 3. Due to its transmission nature, resource limitation of sensor nodes and deployment in uncontrolled environments, the WSN is susceptible to many attacks. Many crypto-mechanisms, such as symmetric and asymmetric methods, are proposed to ensure the security services in WSN. In order to achieve security in without wire sensor networks, it is important that messages sent between sensor nodes are encrypted and authenticated.

Table 3. Security Services.

Services	Description
Confidentiality	The information about the node is kept secret for others while the legitimate users can view the same.
Integrity	To ensure at the receiver end that the message is changed in between.
Device Authentication	Proper explanation for the device identity
Message Authentication	Proper explanation for the data of the source end
Validation	To furnish correctness of authorization to use or manipulate resources.
Access Control	The access to the supports is limited.
Revocation	Renunciation of certification or authorization.
Survivability	In the case when the node is attacked then also the life time of the same should be

	ensured.
Non-repudiation	Preventing the renege of a previous commitment.
Availability	In the WSN framework the all-time available is the desire of the design so that the services are available when looked at, which can be because of the factors like power available, hardware failure, system updations.
Data freshness	Data freshness goal ensures about the freshness of the packet received at the receiver end, meaning ensuring that the received message is not previously used.

3. Literature Survey

Quantity Brownfield, Gupta and Davis, (2005) [32] projected different MAC protocol which moderates various effects of DoS attacks (renege of sleep) by integrating group management. MAC has numerous power redeeming characteristics and is not only increase the network lifecycle, but the central structure proves the network life quite resilient for DoS. Apart from particular period and synchronization text, there exist two different period contention and diverse networks for sharing the message within the groups and outside the group through the gateway node. The MAC protocol enactment outcomes show that G-MAC presents meaningfully over the other available protocols in all traffic conditions. The blank network case marks the protocol overhead and idle listening effects is better depicted with effectual duty cycle-MAC has .95% duty cycle is weighted average of duty cycle of gateway node and other nodes. Intruder can gain admittance to network throughout gateway node. But intruder may only disturb single node at once as the nodes are considered alternatively for the gate way responsibilities centered upon incremental upsurge in power levels.

Brownfield, Gupta and Davis (2005) for the prevention of the DoS attack while broadcasting author M. Brownfield et al., presented a protocol for sleep/listen mac termed as G-MAC. For the purpose of the collection of the traffic and also for forwarding it from the cluster a gateway node is being selected. The gateway node selected only listens to the cluster nodes and before distributing the message over the network the message is needed to be authenticated prior of sending it for broadcasting or even for unicasting. The gateway node is responsible for authenticating the requests of broadcast prior of sending the message to other nodes in the communication or in cluster, which results in the power loss of the gateway node in the authentication process.

Raymond, Marchany, Brownfield and Midkiff (2008)[33] has classified the DoS with respect to the attacker's knowledge about the MAC protocol layer and also with respect to the capability of accessing the authentication and encryption level of the network. A modelling is being done on four different MAC protocols as Sensor MAC (SMAC),Timeout MAC (T-MAC), Berkeley MAC (B-MAC), and Gateway MAC (G-MAC).Executions of particular attacks on MAC, T-MAC, and B-MAC are explained and examined in brief to authenticate their efficacy and examine their effectiveness. As per the analysis it is quite clear that some attacks keep the nodes awake up to 100% in the case when they are in sleep mode for 99% of their life spam, on S-MAC.

Chen Hui, Pei, Ning and Qingquan (2009)[34] considered a method for the fake schedule with RSSI measurement aids. On the basis of the attacks in the past on the network the fake schedules are provided to the nodes in the network. By this method the chances of attacks on the network can be reduced as the network is having the proper schedule all the time and also the attackers may lose their power in attempting for the attack over and over again and may sometime go to dead condition. The health of the network is being considered or even assured when talking about the energy price and the delay of network, using the techniques reduces the packet drop ratio as compared to other techniques without having the fake schedules. In this particular work author have only considered S-MAC protocol with 10% enhancement in duty cycle. The fake scheduling may harmful sometime in the case when there is no data packet loss. RSSI actually is being used as the single value considered for every of the node and also of those node which are having invader one hop away are defined with greater RSSI value.

Riener and Hans-Joachim (2009)[35] described a technique for secure wake up scheme in which a token facility is been provided to all nodes in sleep node to wake up. The disadvantages of the IEEE 802.15.4 standard for transmission are also considered to overcome the sleep deprivation attacks. A secure wake up radio is being utilized to wake up the sleeping node in the case when the message from the authentic and genuine node is in waiting state.

Hoeller, Reinke, Neumann and Groppe (2011)[36] With respect to the introduced fake schedule the attacker will consider the same as original and will create a new duty cycle. As a result of which the attacker node will exhaust its energy in estimation and another task performing. In the above proposal the author has considered that

the attackers' nodes are prepared with less power resources which can also be denied sometimes. The overhead of the network is increased by replacing the fake schedule in generation and in broadcasting.

Gabrielli, Mancini, Setia and Jajodia (2011) [37] have presented a technique to secure the network from the DoS attacks which are actually the counters based on authentication, generally for three following protocols (PEAS, CCP, and ASCENT). The neighbor node may have the shared pair type of key and also can also share with each other. MACs are being generated using the shared pair key, which is then used for the authentication of the unicast of the message in neighboring nodes. The transmission between the neighbors can be hence prevented using the above presented technique.

Hsueh, Wen and Ouyang (2015)[38] proposed a framework; in this work author consider the power exhausting attacks in WSN to resolve the issue of lifetime of node(s) or complete network. For secure mechanism author consider SATCA to create a hierarchical topology, it has four following stages as Anti-Node Investigate**,** group formation**,** Key distribution**,** Key renewal.

4. Problem Formulation

In the growing global requirements, the WSN has its own importance in all available fields in the physical world. Other than sensing the low power mode the sensors are being used many other applications for many purposes like temperature detection, pressure detection and also pollution detection. So as to save the energy of the sensor nodes, constrained set them in sleep state most of the time, which also increases the life spam of the nodes. The DoS are the attacks which make the nodes to be in the state of wake up and effects the life span of the nodes. So, in this research we planned a framework for the solution of such type of attacks through the detection of anti or malicious node.

For finding security in WSN, the security parameter of the recommended path will be calculated, the state of having malicious node will be roughly calculated in the accepted circumstances which will be used for the results appraisal. The RSSI value and the information about the routing will be combined together for the detection of the nodes which are malicious and also goes for checking the attacker's identity. During the initial stage of the transmission there will be a proper establishment of the path for routing and also for the computation of the RSSI values and recording the same. After that network confirms each and every node about the strength of packet from the side of the source node. In the case when the RSSI value is not equal to the signal strength of the data packet that means the network has detected a malicious node and for the security of data packet will be encrypted with a private key.

The energy or power of a sensor node(s) and security issue in WSN is important as it supports in defining how likely a network is considered for future communication as it assists in preserving the complete lifespan and accurateness of WSN system.

5. Objective Of The Work

The main Objective of the study are as under:

- To study the in-depth information about WSN and related attacks,
- To study and evaluate the different energy exhausting attacks,
- To formularize a solution for power exhausting attack based on literature presented,
- To present a study and evaluation of the presented technique.

6. Methodology To Be Adopted

In the proposed research work a framework is proposed for power exhausting attacks in WSN. In the growing global requirements, the WSN has its own importance in all available fields in the physical world. Other than sensing the low power mode, the sensors are being used in many other applications for many purposes like temperature detection, pressure detection and also pollution detection. So as to reduce the energy usage of the sensor nodes the constrained set them in sleep state most of the time, which also increases the life span of the nodes. The DoS are the attacks which make the nodes to be in the wake-up state and effects the life span of the nodes. So, in this research the framework is planned for the solution of such type of attacks through the detection of anti or malicious node.

It is proposed to extend the work carried out, to minimize the overhead and improve the security parameter for a same type of attacks in WSN. Key renewal phase creates maximum overhead because key renewal means every time key is generated and delivered so to minimize the overhead, the key renewal phase is not counted and to maintain the security parameter RSSI (Receiving Signal Strength Indicator) value is considered.

In nutshell the proposed work shall be carried out in the following phases:

1. **Anti-node detection phase: -** Encrypted hello messages are broadcasted along with the RSSI value and in the case when the sensor node is not able to decrypt the hello message and also the when the RSSI value and signal strength mismatches, proves the detection of anti-note.
2. **Cluster formation: -** Group of nodes with similar characteristics is group, group head is selected on the basis of waiting timer for broadcasting the hello message and listening to the same from neighbor and also power is considered for assigning any node as cluster head.
3. **Key distribution: -** The two-way symmetric key is generated and broadcasted by cluster head for the decryption of the hello messages broadcasted, hence cluster head is supposed to be good in power.

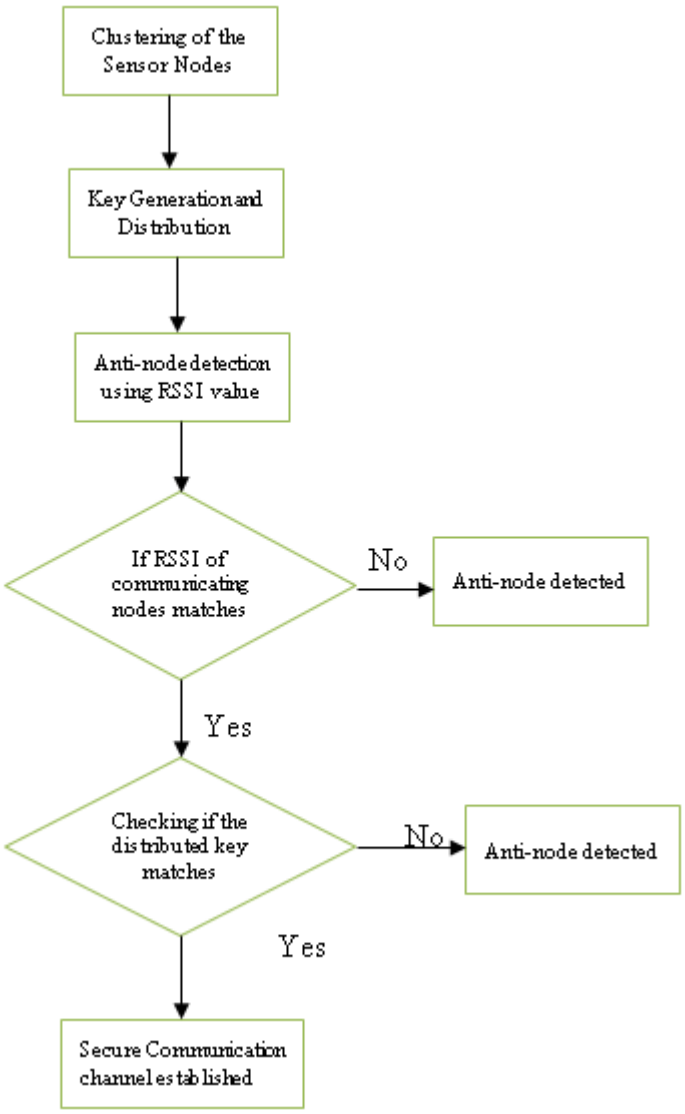

Figure 6. Block diagram of Research Methodology.

7. Expected Outcomes Of The Research

The RSSI value and the information about the routing is being combined together for the detection of the nodes which are malicious and also goes for checking the attacker's identity. During the initial stage of the transmission there is a proper establishment of the path for routing and also for the computation of the RSSI values and recording the same. After that every node in the network confirms about the packet strength from the side of the source node. In the case when the RSSI value is not equal to the signal strength of the data packet that means the network has detected a malicious node. And for the security of data packet encryption using a private key is considered.

The energy or power of a sensing node(s) and security issue in WSN is important as it supports in defining how likely a network is utilized for future communication. It assists in preserving the complete life and accurateness of the WSN system.

For qualitative outcomes, the proposed methodology is to be tested considering certain parameters like: Security, utilization, time interval, traffic overhead so as to compare the performance related parameters, the outcomes of proposed methodology will be compared with existing approach by (Hsueh, Wen and Ouyang, 2015). The outcomes will describe that the proposed methodology will enhance the prevention of renege of sleep attack and security of the sensor network. It is expected that the proposed work shall result in higher security with low overhead.

8. Conclusion And Future Direction

The current work describes the brief introduction about the WSN and related characteristics and foremost issues and challenges. After considering various related issues and challenges of the domain the major considered segment is about the power management for the sensor nodes. In majority of the works the major concern is about the extra power exhausted because of some unwanted processing's like DoS (Denial of Sleep), which actually is the category of attack which keeps the nodes awake most of the time without any usage of the same in the current communication to exhaust the power of the sensor nodes. In the work presented the literature review is also conducted for the better understanding the of the problem and also for the better formulation of the problem which results in the power exhausting. In the growing global requirements, the WSN has its own importance in all available fields in the physical world. Other than sensing the low power mode the sensors are being used many other applications for many purposes like temperature detection, pressure detection and also pollution detection. So as to save the energy of the sensor nodes, constrained set them in sleep state most of the time, which also increases the life spam of the nodes. The DoS are the attacks which make the nodes to be in the state of wake up and effects the life period of the nodes. In the present work on the basis of the problem formulated relying over the considered literature review a specific power management scheme is presented which uses RSSI and encryption techniques for security and for power management to resist the network to loss the power and also for the Investigate and malicious nodes. The works presented the ways via which the proposed techniques is to be validated to generate better results. The work focuses more over the background study and solution to the problem formulated which can be further considered for validation part considering some of the real-time simulation platforms like NS2/MATLAB, for better validation of the work presented..

References

1. Akkaya, Kemal, and Mohamed Younis. "A survey on routing protocols for wireless sensor networks." Ad hoc networks 3.3 (2005): 325-349.
2. Buratti, Chiara, et al. "An overview on wireless sensor networks technology and evolution." Sensors 9.9 (2009): 6869-6896.
3. Wang, Yu. "Topology control for wireless sensor networks." Wireless sensor networks and applications. Springer, Boston, MA, 2008. 113-147.
4. Chen, Xiao, and Neil C. Rowe. "An Energy-Efficient Communication Scheme in Wireless Cable Sensor Networks." 2011 IEEE International Conference on Communications (ICC). IEEE, 2011.
5. Cheng, Chi-Tsun, K. Tse Chi, and Francis CM Lau. "A delay-aware data collection network structure for wireless sensor networks." IEEE sensors journal 11.3 (2010): 699-710.
6. Matin, Mohammad Abdul, and M. M. Islam. "Overview of wireless sensor network." Wireless Sensor Networks-Technology and Protocols (2012): 1-3.
7. Paul, Biswajit, and Mohammad Abdul Matin. "Optimal geometrical sink location estimation for two-tiered wireless sensor networks." IET wireless sensor systems 1.2 (2011): 74-84.
8. Fabbri, Flavio, et al. "Area throughput and energy consumption for clustered wireless sensor networks." 2009 IEEE Wireless Communications and Networking Conference. IEEE, 2009.
9. Akyildiz, Ian F., et al. "Wireless sensor networks: a survey." Computer networks 38.4 (2002): 393-422.
10. Bharathidasan, A. R. C. H. A. N. A., V. Anand, and S. Ponduru. "Sensor Networks: An Overview, Department of Computer Science, University of California." DAVIS, CA 95616 (2001)..
11. Yick, Jennifer, Biswanath Mukherjee, and Dipak Ghosal. "Wireless sensor network survey." Computer networks 52.12 (2008): 2292-2330.
12. Boukerche, Azzedine, ed. Algorithms and protocols for wireless and mobile ad hoc networks. Vol. 77. John Wiley & Sons, 2008..

13. Sohraby, Kazem, Daniel Minoli, and Taieb Znati. Wireless sensor networks: technology, protocols, and applications. John wiley & sons, 2007.
14. Verdone, Roberto, et al. Wireless sensor and actuator networks: technologies, analysis and design. Academic Press, 2010.
15. Aziz, Nor Azlina Ab, and Kamarulzaman Ab Aziz. "Managing disaster with wireless sensor networks." 13th International Conference on Advanced Communication Technology (ICACT2011). IEEE, 2011.
16. Boyle, David, and Thomas Newe. "Securing Wireless Sensor Networks: Security Architectures." J. Networks 3.1 (2008): 65-77.
17. Hu, Fei, and Neeraj K. Sharma. "Security considerations in ad hoc sensor networks." Ad Hoc Networks 3.1 (2005): 69-89.
18. Walters, John Paul, et al. "Wireless sensor network security: A survey." Security in distributed, grid, mobile, and pervasive computing 1.367 (2007): 6.
19. Anjum, Farooq, and Saswati Sarkar. "Security in sensor networks." Mobile, Wireless, and Sensor Networks (2006): 283..
20. Perrig, Adrian, John Stankovic, and David Wagner. "Security in wireless sensor networks." Communications of the ACM 47.6 (2004): 53-57.
21. Karlof, Chris, and David Wagner. "Secure routing in wireless sensor networks: Attacks and countermeasures." Ad hoc networks 1.2-3 (2003): 293-315..
22. Newsome, James, et al. "The sybil attack in sensor networks: analysis & defenses." Third international symposium on information processing in sensor networks, 2004. IPSN 2004. IEEE, 2004.
23. Younis, Ossama, and Sonia Fahmy. "HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks." IEEE Transactions on mobile computing 3.4 (2004): 366-379.
24. Pan, J., Hou, Y.,Chai, L., Shi, Y., & Shen, S. (2003). Topology Control for Wireless Sensor Networks. Proc. 9th ACM Int. Conf. on Mobile Computing and Networking, San Diego, USA, September, 286-29.
25. Zeng, Xiang, Rajive Bagrodia, and Mario Gerla. "GloMoSim: a library for parallel simulation of large-scale wireless networks." Proceedings. Twelfth Workshop on Parallel and Distributed Simulation PADS'98 (Cat. No. 98TB100233). IEEE, 1998.
26. Ye, Wei, John Heidemann, and Deborah Estrin. "Medium access control with coordinated adaptive sleeping for wireless sensor networks." IEEE/ACM Transactions on networking 12.3 (2004): 493-506.
27. Van Dam, Tijs, and Koen Langendoen. "An adaptive energy-efficient MAC protocol for wireless sensor networks." Proceedings of the 1st international conference on Embedded networked sensor systems. 2003.
28. Polastre, Joseph, Jason Hill, and David Culler. "Versatile low power media access for wireless sensor networks." Proceedings of the 2nd international conference on Embedded networked sensor systems. 2004.
29. Raymond, David R., et al. "Effects of denial-of-sleep attacks on wireless sensor network MAC protocols." IEEE transactions on vehicular technology 58.1 (2008): 367-380.
30. Chen, Chen, et al. "An effective scheme for defending denial-of-sleep attack in wireless sensor networks." 2009 Fifth International Conference on Information Assurance and Security. Vol. 2. IEEE, 2009.
31. Pawar, Pranav M., et al. "GHMAC: Green and hybrid medium access control for wireless sensor networks." Wireless Personal Communications 94.3 (2017): 1839-1868.
32. Kaur, Simerpreet, and Md Ataullah. "Securing the wireless sensor network from denial of sleep attack by isolating the nodes." International Journal of Computer Applications 103.1 (2014).
33. Raymond, David R., et al. "Effects of denial-of-sleep attacks on wireless sensor network MAC protocols." IEEE transactions on vehicular technology 58.1 (2008): 367-380.
34. Chen, Chen, et al. "An effective scheme for defending denial-of-sleep attack in wireless sensor networks." 2009 Fifth International Conference on Information Assurance and Security. Vol. 2. IEEE, 2009.
35. Falk, Rainer, and Hans-Joachim Hof. "Fighting insomnia: A secure wake-up scheme for wireless sensor networks." 2009 Third International Conference on Emerging Security Information, Systems and Technologies. IEEE, 2009.

36. Hoeller, Nils, et al. "Dynamic Approximative Caching Scheme for energy conservation in Wireless Sensor Networks." Journal of Networking Technology Volume 2.1 (2011): 11.
37. Gabrielli, Andrea, et al. "Securing topology maintenance protocols for sensor networks." IEEE Transactions on Dependable and Secure Computing 8.3 (2010): 450-465.
38. Hsueh, Ching-Tsung, Chih-Yu Wen, and Yen-Chieh Ouyang. "A secure scheme against power exhausting attacks in hierarchical wireless sensor networks." IEEE Sensors journal 15.6 (2015): 3590-3602.