International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Email:editorijoer@gmail.com http://www.ijoer.in

Vol.4., Issue.1., 2016
(Jan-Feb)

REVIEW ARTICLE

ISSN: 2321-7758

# PREVENTING SLEEP DEPRIVATION TORTURE ATTACK IN WIRELESS SENSOR NETWORK USING SENSOR MONITOR ALGORITHM

**ABDUL REHMAN AFRAD[1], VEENA PATIL[2]**
[1]Assistant professor department of Computer Science and Engineering,
Secab Institute of Engineering & Technology, Vijayapur, Karnataka, Nauraspur, Bagalkot road ,vijayapur, Karnataka,India
[2]Department of Computer Science and Engineering, Secab Institute of Engineering & Technology, Vijayapur, Karnataka, Naurasarpur,Bagalkot raod,Vijayapur, Karnataka,India

ABDUL REHMAN AFRAD

VEENA PATIL

**ABSTRACT**

The Optimized Link State Routing Protocol (OLSR) is an IP routing protocol optimized for mobile ad hoc networks, and also used on other wireless ad hoc networks. OLSR uses 2 types of control messages; Hello and Topology Control (TC). Both the type of messages are un-authenticated hence, OLSR is susceptible to numerous attacks specifically, black hole, worm hole, gray hole etc. The present paper focuses on Sleep Deprivation Torture Attack on OLSR. In Sleep deprivation attack in layer 2, the attacker tries to use a small energy node till all its energy is exhausted and the node goes into stable sleep. This type of attack can also takes place in routing level. In OLSR small energy node declares their status through willingness property of HELLO message. With the help of this information an attacker node can select that small energy node deliberately and promote all traffic through that node. This leads to small energy node in a stable sleep mode.

**Keywords**— Wireless Sensor Network, Optimized Link State routing (OLSR), Sleep Deprivation.

## I. INTRODUCTION

A wireless sensor network (WSN) generally consists of a base station that can communicate with a number of wireless sensors via a radio link. In WSN, a large number of tiny sensor nodes are densely placed in a sensor field and sensor nodes collect data and transmit directly to the gateway. Forest fire detection, flood detection, military purposes, child education, tracking and monitoring doctors and patients inside a hospital, micro-surgery, home application, commercial application are various types of possible applicability of WSNs. WSNs provide lots of opportunities, at the same time, link breakage, node failure happen quite frequently. Routing can face those challenges. Proactive routing protocol and reactive routing protocol are two main types of routing protocol in WSNs. Proactive protocols find the paths for all source and destination pairs in advance, whereas, reactive protocols search a route only when there are data to be transmitted. Optimized Link State Routing (OLSR) is one of very popular proactive routing protocol. A fresh routing table of destination nodes and their paths are always maintained by OLSR. Routing tables are updated whenever there is any change in network.

Intrusions can be imposed from different directions on network environments. Particularly on Mobile ad hoc Networks (MANETs), it is more frequent as the nature of this network is exposed it to be attacked. This happens due to the lack of defined infrastructures i.e uses wireless media and it has no defined perimeters and the communication medium used is not trusted; the mobility of the nodes can create additional problems on management of the topology of the network. These properties of MANET increased its susceptibility to intrusions. To address these problems there are several approaches proposed by different researchers. In this approach additional message for verification of the path, detection and isolation is used to test the validity of the route. Strong security mechanism should be developed to understand the nature of the normal nodes and malicious nodes so as to develop the detection mechanism. MANETs uses different routing protocol for communications to maintain the network and Optimized Link State Routing (OLSR) protocol is one of those protocols. Optimized Link State Routing (OLSR) is a standard proactive routing protocol for Wireless Sensor Network (WSN). OLSR uses two kinds of the control messages: Hello and Topology Control (TC). As these messages are un-authenticated, OLSR is prone to several attacks namely, blackhole, wormhole, grayhole etc. This paper is focused at Sleep Deprivation Torture Attack on OLSR. Sleep deprivation attack is one of the most interesting attack in layer 2 where the attacker tries to use a low energy node until all its energy is exhausted and the node goes into permanent sleep. This attack is also possible in routing level. In OLSR low energy node declare their status through willingness property of HELLO message. Using this information an attacker node can choose that low energy node deliberately and forward all traffic through that node. This leads to low energy node in a permanent sleep mode.

## II.LITERATURE SURVEY

**De Rango, Floriano et. Al. [1]:**presents Ad-hoc networks have to suffer many challenges at the time of routing. Dynamically changing topology and no centralized infrastructure are the biggest challenges in the designing of an Ad hoc network. The position of the nodes in an Ad-hoc network continuously varies due to which we can't say that any particular protocol will give the best performance in each and every case topology varies very frequently so we have to select a protocol which dynamically adapts the ever-changing topology very easily. Another challenge in MANET is limited bandwidth. If we compare it to the wired network then wireless network has less and more varying bandwidth, so bandwidth efficiency is also a major concern in Ad-hoc network routing protocols. Limited power supply is the biggest challenge of an Ad-hoc network so if we want to increase the network lifetime (time duration when the first node of the network runs out of energy) as well the node lifetime then we must have an efficient energy management protocol. So an Ad-hoc routing protocol must meet all these challenges to give the average performance in every case. MANET (Mobile Ad hoc Network) is a self organizing and self configuring network without the need of any centralized base station. It is a collection of nodes that is connected through a wireless medium forming rapidly changing topologies. MANETs are infrastructure less and can be set up anytime, anywhere. In MANETs, the nodes are mobile and battery operated. As the nodes have limited battery resources and multi hop routes are used over a changing network environment due to node mobility, it requires energy efficient routing protocols to limit the power consumption, prolong the battery life and to improve the robustness of the system.

This paper evaluates the performance of various ad hoc routing protocols such as DSDV, AODV, and DSR in terms of energy efficiency by varying pause time, node velocity and packet sending rate.. Simulation is done using NS-2(version NS-2.34). It has been verified through extensive simulations, which represent a wide spectrum of network conditions that AODV delivers the better performance as that of the state-of the- art algorithms DSDV and DSDV but it is observed that DSR needs significantly smaller energy expenditure than AODV and DSDV.

**Nune Sreenivas et. Al [2]:** paper presents Detection Mechanism on OLSR Protocol This work focuses only on traffic relay/generation refusal where the malicious node acts as a black-hole and drops packets. Two types of attackers are introduced in this study where the first type is the malicious node which drops all the received packets and the second attacker type is the malicious node which is smarter than the first type and drops only data packets and exchanges control packets normally. To detect and isolate these attackers we need to extend the security of OLSR protocol in order to minimize their effects by working on two different aspects. The first security aspect validates the communication path by sending periodic messages and the second aspect is concerned with finding malicious node in the invalid path so that any other measure to make the communication line can be taken.

**Ian F. Akyildiz et.al, [3]:** provides a survey of Wireless Sensor Networks Issues and Applications, where the use of such sensor networks has been proposed. Wireless Sensor Networks have come to the forefront of the scientific community recently. Current WSNs typically communicate directly with a centralized controller or satellite. On the other hand, a smart WSN consists of a number of sensors spread across a geographical area; each sensor has wireless communication capability and sufficient intelligence for signal processing and networking of the data. The structures of WSNs are tightly application-dependent, and many services are also dependent on application semantics. Thus, there is no single typical WSN application, and dependency on applications is higher than in traditional distributed applications. The application/middleware layer must provide functions that create effective new capabilities for efficient extraction, manipulation, transport, and representation of information derived from sensor data.

**Tapalina Bhattasali et.al, [4]:** mainly focuses on sleep deprivation attack which is also considered as layer 2 attack. This section gives an idea about the related mitigation technique of it. The network lifetimes of existing Medium Access Control (MAC) protocols such as Sensor MAC (S-MAC), Timeout MAC (T-MAC) and Berkley MAC (B-MAC) were compared by Raymond et.. Brownfield et. al. had proposed a protocol Gateway MAC to mitigate the effects of denial of sleep attacks. WSNET link layer protocol G-MAC can serve as an effective denial of sleep defense by centralizing cluster management. Our research focuses on distributed anomaly detection technique in order to provide a reliable and energy efficient heterogeneous wireless sensor network. Anomaly is detected by comparing the values with predefined parameters specified in normal profile. The proposed model uses anomaly detection technique in such a way so that false intrusion detection can be avoided. To mitigate the attack, proposed model physically excludes malicious nodes from the network and rejects fake packets.

**Xu Ning and Christo G. Cassandras [5]** considered a sender-receiver link in a WSN. The sender is a wireless node equipped with some event detector which is driven by external, random events such as body movements in a room or fire alarms. When the sender detects an event or reports its status, it sends a message to the receiver, which is a downstream node in the network. In this link, variable preamble LPL is used. Depending on the specific application, LPL can have different implementations. The formulated a dynamic optimization problem for saving energy in a transmission control scheme based on a variable preamble technique. The first managed to solve the continuous time Bellman equation, resulting in a pair of differential equations characterizing the optimal solution. Since the differential equations, although efficient to solve, provide only necessary optimality conditions and do not always lead to global optimal solutions, the system and provided the DP algorithm which is easy to implement and low in complexity. Our numerical results show that our approach fully utilizes statistical information in controlling the sleep time of a wireless sensor node, resulting in substantial energy savings in comparison to the best possible fixed sleep time control.

## III.EXISTING SYSTEM

### 3.1 Energy Efficient OLSR:

Energy is an important parameter in case of wireless sensor networks because sensor nodes are small in size and has limited battery backup. Also, nodes can continuously move in an uncontrolled manner, so frequent route failures are possible. The solution of these issues of WSN is energy efficient routing. Energy efficiency is not only the measurement of power consumption at a given time. It is actually the duration of the time over which the network can maintain a certain performance level, which is usually called as the network lifetime. In this attack, the attacker applies the reverse philosophy which is used to make the OLSR energy efficient. To elaborate, in energy efficient in OLSR, a node selects its MPR which has the maximum remaining energy among all possible MPRs. In case of the attack, the attacker node does the reverse and selects the MPR which has the minimum energy remaining.

In EE-OLSR, MPR (multipoint relays) nodes are selected only based on their willingness property which normally shows the battery life time of a node. But EE-OLSR is unaware about unauthorized access.

**Disadvantages of Existing System:**

- Unaware about unauthorized access.
- Nodes can continuously move in an uncontrolled manner, so frequent route failures are possible.
- Limited battery backup.

## IV.PROPOSED SYSTEM

Intrusion is any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource; whereas IDS are a system for the detection of such intrusions. Intrusion detection for MANETs is a complex and difficult task mainly due to the dynamic nature of MANETs, their highly constrained nodes, and the lack of central monitoring points. WSNs is a collection of few number of sensor nodes. Sensor Monitors (SMs) [15] are nothing but a special kind of more powerful sensors. SMs observe the entire situation and as per the requirement, it tries to store HELLO and TC messages in different tables. Finally SMs communicate with other SMs and match different situations and try to detect unauthorized access. So IDS is executed inside of the SMs. Sensor nodes are grouped to form clusters monitored by SMs individually.

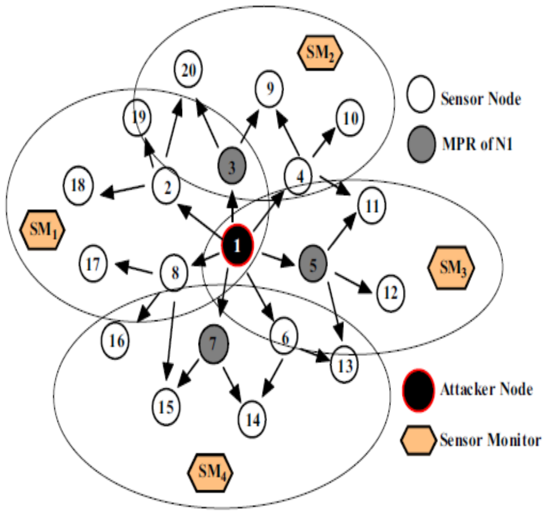

**Fig 4.1: Example Scenario of wireless sensor networks with monitor**

This subsection illustrates the scheme with an example of a simple WSN (Fig.1). In Fig.1, SM1, SM2, SM3, SM4 are sensor monitors and one SM covers sensor nodes within its range. {N2, N3, N4, N5, N6, N7, N8} are the 1-hop neighbours of node N1 and {N9, N10, N11, N12, N13, N14, N15, N16, N17, N18, N19, N20} are 2-hop neighbours of N1. HELLO messages are broadcasted by N2, N3, N4, N5, N6, N7 and N8 and these HELLO messages are stored in HELLO table of SM1, SM2, SM3 and SM4. For willingness N2, N3, N4, N5, N6, N7 and N8 declared integer values 7, 1, 6, 1, 6, 1, 6 respectively through their HELLO messages.

**Advantages of Proposed System:**

- Good throughput.
- OLSR minimizes the overhead from flooding of control packets by using only a subset of its neighbour nodes, called multipoint relays (MPRs)
- HELLO messages are broad-casted after a certain interval to trace neighbours and maintain communication with them.

## CONCLUSION

Energy efficient OLSR is a prime contribution in the field of WSN. This is a novel energy aware MPR election policy. EE-OLSR outperforms traditional OLSR in terms of throughput, packet delivery ratio, end-to end delay, average nodes lifetime etc. However, EE-OLSR does not check authenticity of packets and therefore many attacks, like sleep deprivation is possible on EE-OLSR. Sleep deprivation attack is one of the most interesting attack in layer 2 where the attacker tries to use a low energy node until all its energy is exhausted and the node goes into permanent sleep. This attack is also possible in routing level. In OLSR low energy node declare their status through willingness property of HELLO message. Using this information an attacker node can choose that low energy node deliberately and forward all traffic through that node. This leads to low energy node in a permanent sleep mode. The performance of the propose algorithm is studied by Network Simulator (NS2) and effectiveness of the propose scheme, along with a comparison with existing techniques is demonstrated. Experimental results illustrated that the IDS can successfully nullify the effect of the attack to a great extent in terms of throughput, PDR, end-to-end delay and average node lifetime.

## REFERENCES

[1]. De Rango, Floriano, Marco Fotino, and Salvatore Marano. "EE-OLSR: energy efficient OLSR routing protocol for mobile ad-hoc networks." IEEE Military Communications Conference, 2008.

[2]. Nune Sreenivas1, P.G.V.Suresh Kumar " Detection and Segregation of Misbehavior Node(S) for MANETS OLSR Protocol" Volume 3, Issue 11, November 2014

[3]. Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci "A Survey on Sensor Networks", IEEE Communications Magazine, vol. 40, no.8, pp. 102–114, August 2002.

[4]. Tapalina Bhattasali, Rituparna Chaki, Sugata sanyal (2012): "Sleep deprivation Attack Detection in Wireless Sensor network", International Journal of Computer Applications, Feb. 2012.

[5]. Xu Ning and Christo G. Cassandras (2008): "Optimal Dynamic Sleep Time Control in Wireless Sensor Networks", IEEE Conference on Decision and Control Cancun, Mexico, Dec. 2008.