International Research Journal of Computer Science (IRJCS)
Issue 11, Volume 4 (November 2017)
ISSN: 2393-9842
www.irjcs.com

A STUDY AND COMPARATIVE ANALYSIS OF POWER EXHAUSTING ATTACK

Jaya Kaushik
Department of Electronics and Communication,
Manav Rachna International University, Faridabad, India
Er.jayakaushik15@gmail.com

Dr. Naresh Grover
Department of Electronics and communication,
Manav Rachna International University, Faridabad, India
dean.academics@mriu.edu.in

Manuscript History
Number: **IRJCS/RS/Vol.04/Issue11/SPCS10084**
DOI: 10.26562/IRJCS.2017.SPCS10084
Received: 08, September 2017
Final Correction: 12, October 2017
Final Accepted: 03, November 2017
Published: November 2017
Citation:

Editor: Dr.A.Arul L.S, Chief Editor, IRJCS, AM Publications, India

Abstract— The communication network where there is no requirement of infrastructure is termed as the wireless network. In wireless mode of communication the sensor nodes are established and provides help to the other sensor nodes directly or indirectly, the nodes available in the wireless network can play the role of the router or can work as the single node. There exist a wide range of applications of wireless network in today's communication scenario, as wide range of the applications are being supported by the wireless network which makes it more suitable and also due the decentralized facility provided by the network. The scalability of the network is increased as compared to the networks which are being supported by the wireless network, it is quite easy to identify the limitations of the network either the theoretical one or the practical one. The radio communication is being used for the administration and also for the implementation of the wireless network. The protection of information for long period time is very critical in many environments. Power is the most important concern for data transfer between wireless nodes. In this paper, we concern on the denial of sleep attack issue in WSN and also reviewed some of the methodologies for the same; DoS that targets a battery powered device's power supply in an effort to exhaust this constrained resource and reduce the network life time.

Keywords - Wireless Sensor Network, Communication, Power Consumption, Deniel Of Service, ad-hoc.

I. INTRODUCTION

Wireless sensor network is a communication infrastructure between nodes. In wireless mode of communication the sensor nodes are connected and provide help to the other sensor nodes directly or indirectly, the nodes available in the wireless network can play the role of the router or can work as the single node. As the wireless network is completely infrastructure less and hence for the communication between the autonomous nodes available in the network there is no need of any defined infrastructure.

The infrastructure of the network is dynamic and hence it easy to add new sensor nodes and also to delete the nodes in the network. Wireless sensor network is a self-configuring, infrastructure less and dynamic topology. Communication network is the combination of several nodes for the effective communication hence the nodes are to be connected using the cables in the home network or in the enterprises which is quite costly hence the wireless network provides the connection free environment for the effective communication network. The radio communication is being used for the administration and also for the implementation of the wireless network. The protection of information [1] [2] for long period time is very critical in many environments. Power is the most important concern for communicate between wireless nodes. MANET (Mobile Ad hoc Network) in early 1970s is known as packet radio network the complete project was sponsored by DARPA (Defense Advanced research Agency). The project was to provide communication between the several nodes in the conditions like war and project was named as packet radio. The main motivation behind the original internet protocol suite was the packet radio system at that time which also predicted the Internet. The life cycle of the Ad hoc Network goes like first generation, second and third generation of the Ad hoc Network systems. The present communication system used for the communication is the third generation of the Ad hoc Network systems. Packet Radio Network (PRNET) was the first generation communication network in around 1972. In conjunction with ALOHA (Arial Locations of Hazardous Atmospheres) and CSMA (Carrier Sense Medium Access), approaches for medium access control and a kind of distance-vector routing PRNET were used on a trial basis to provide different networking capabilities in a combat environment.

1980 was the time for the second generation wireless communication network system, where the first generation network was enhanced and implemented as Survivable Adaptive Radio Network (SURAN). The second generation of the wireless network has provided the packet switched network where there was no need of the infrastructure for the communication in the battlefield. The second generation system for the wireless network was beneficent because of the facilities like resilience to the electronic attacks and was cheaper and smaller as compared to the first generation systems by which the performance of the radio network was improved.

There exists wide range of applications of the wireless network like exchange of information in the conditions like war and also in the condition of emergency exchange of information like in hospital and in the areas of the disaster. The wireless communication is also used in the robot acquisition system for the purpose of the information exchanging. Another wide application area of the wireless network is the field of entertainment for sharing the various aspects of the entertainment like games, music, videos, data, etc. The wireless communication network has its wide use in the field of the education so that the various study material can be archived. The critical information is being exchanged in the case of the surveillance system using the wireless communication system.

There are various types of wireless network [3] which are used in different place with different users.

- Wireless local area networks,
- Wireless personal area network,
- Wireless metropolitan area network,
- Wireless wide area network.

TABLE I: UPDATION TECHNIQUES IN WIRELESS NETWORK.

Type	Coverage	Performance	Standards	Application
Wireless PAN	Within reach of a person	Moderate	Wireless PAN Within reach of a person Moderate Bluetooth, IEEE 802.15, and IrDA Cable replacement for peripherals.	Cable replacement for peripherals
Wireless LAN	Within a building or campus	High	IEEE 802.11, Wi-Fi, and Hiper LAN	Mobile extension of wired networks
Wireless MAN	Within a city	High	Proprietary, IEEE 802.16, and WIMAX	Fixed wireless between homes and businesses and the Internet
Wireless WAN	Worldwide	Low	CDPD and Cellular 2G, 2.5G, and 3G	Mobile access to the Internet from outdoor areas

II. ISSUES AND CHALLENGES

There are five major implications and challenges of wireless networks as under:

- **Security-** There is chance of data fraud, ultration of data and the destruction and even replacement of the various sensor nodes in the wireless communication network system.
- **Hidden Terminal Problem-** In the case of the three way communication there chance of data collision at the end of the receiver for example A, B and C are three different nodes in the network and the node A and B are sending the data to the node C hence the node B is hidden for the node A.
- **Expose Terminal Problem-** Suppose X is busy doing transmission with W. At the same time Y wants to start the transmission with another node Z but Y is not able to start the transmission because W incorrectly sense medium is busy.
- **Selection of Transmission Rate-** As the wireless communication network is infrastureless and hence for the sending the data from one node to another it is quite necessary to define the transmission rate of the data sending between two communicating nodes without any interferance of the third node in the same network.
- **Power Control-** Power management is very critical in MAC protocol due to collision and packet loses. Challenge of the power control is throughput needs to be maximized and how to select transmission rate of the nodes so that the collision should not occur and also energy management of the nodes too.

III. DIFFERENT TYPES OF ATTACKS IN WSN

1. **Collision Attack**
   As the wireless communication network is infrastructure less means there is no end to end connectivity between the nodes and some malicious node may exist in the network because of which there is a chance of the collision of the data. As the malicious node in the network don't go with the MAC protocols and hence cause collision of the data by sending the noise packets in the network. Due to the fact that the network is having the broadcasting nature hence it is quite hard to detect the collision attacks.

2. **Unintelligent Attack**
   In this type of attacks the lack of knowledge about the MAC protocol which causes the inability in penetrating the network and the past events keep on replaying because of which the nodes fails to go in sleep mode and also result in the wastage of the energy because the node has to receive and process the extra packet receined due to attack.

3. **Unauthenticated Broadcast attack**
   In this type of attacks the attacker has the complete knowledge of the different MAC protocols but it fails to penetrate the wireless network. Just because of the fact that the attacker has the complete knowdge of the MAC protocols hence the attaker just broadcast the unwanted packet in the network and increases the traffic in the network. By the broadcast of the unnecessary traffic in the network the sleep cyle and the listen cycle of the sensor node is being effected, as there is traffic in the network means the nodes are in the listenning mode by which the energy consumption is increased and also it reduces the lifetime of the wireless communication netwrok.

4. **Full Domination attack**
   In this type of attacks the malicious nodes have the complete knowledge of the MAC protocols and also have the ability of the network penetration. The full domination attacks are more destructive as they can produce the trusted traffic in the network and can gain the denial of sleep impact of the node. This kind of attacks enters the network from the one or more nodes in the network which are compromised.

5. **Exhaustion attack**
   In this type of the attacks the attacker have the complete knowledge of the MAC protocols and also has the ability of the hetwork penetration [4]. These attacks are possible only in case of request to send (RTS)/clear to send (CTS) based MAC protocols. In this type of attacks the attacker first sends RTS to the available node in the network and in the case when the node after receieving the RTS responds with the CTS then it keeps on sending the RTS to the node.

6. **Intelligent Jamming attack**
   This type of attacks are one of the most destructive attacks in the wireless communication network as the attacker have the complete knowledge of the MAC protocols but it is not able to penetrate the wireless network. The attacker injects unauthenticated unicast and broadcast packets into the network. These attacks can differentiate between control traffic and data traffic and unlike the unauthenticated replay attack it replays the selective events (control or data).

7. Sleep Deprivation Attack

In this type of attack the attacker tries to increase the energy consumption by any node so that it reduce the total lifetime of the node. The Sleep deprivation attack [5] the attacker just disturbs the sleep cycle of the node so that its power conservation fails, all is done by the means of the lawful interactions. Further, this attack is difficult to detect given that it is carried out solely through the use of seemingly innocent interactions.

8. Barrage Attack

This type of attacks are presented in [6] and the attacker just floods the node by sending the unnecessary RTS, the main motive of the attacker is just to consume the power of the node. Because of the unwanted RTS the attackers just keeps the node out of its sleep cycle. In both the sleep deprivation attack and the barrage attack the victim will never enter its low power sleep mode. The main difference between the barrage attack [6] and the sleep deprivation attack is that the in the case of the barrage attack the attacker is quite active all the time and in the case of the sleep deprivation attack the attack remains idle most of the time.

9. Synchronization Attack

This type of attacks occurs at the MAV layer and causes the problem of relative time synchronization [7]. As the synchronization attacks are with in the confines of the MAC protocols hence they are hard to detect but are simple in nature. In the MAC protocol the sleep and listen schdule is being maintained by each node and the clock drift and the virtual cluster of the neighbouring node is being synchronized by exchanging the sleep-listen schdule periodically. That allows them to listen and go to sleep at the same time. Updating schedule is accomplished by sending a SYNC packet.

10.Replay Attack

A replay attack is a breach of security in which information is stored without authorization and then retransmitted to trick the receiver into energy exhaust operations. In an unintelligent replay attack, recorded traffic is replayed into the network, causing nodes to waste energy receiving and processing these extra packets if nodes in the network do not implement an anti-replay mechanism, this attack causes the replayed traffic to be forwarded through the network, consuming power at each node on the path to the destination.

IV. DIFFERENT PREVENTION METHODOLOGIES FOR ATTACKS IN WSN

This section of the paper illustrates the previous research studies on power exhausting attack in wireless network and reviews some related recent work on its prevention. Brownfield et al. [8] presented a MAC protocol which uses the cluster management which is centralized and many of the denial of sleep attacks are being mitigated by this. The lifetime of the node is more resistant to the sleep denial attacks because of the centralized architecture of the algorithm. Special gateway node is being used for message sending inside the cluster of the node and outside the cluster as well and also maintains different network for message sending and has two contention periods. The analysis of the G-MAC shows that the methodology outperforms over other protocols when performed over the MAC protocol. The protocol overhead is being shown by the empty network case and the effective duty cycles are used for detecting the idle listening effects. MAC has .95% duty cycle is weighted average of duty cycle of gateway node and other nodes. Gateway nodes are breakthrough for the attackers to get entry in the network. As the responsibilities of the gateway nodes are alternated by each node hence the attacker can only make an impact over a single node at a time which is being based on the increasing level of the battery level.

David R. Raymond et al. [9] defines the denial of sleep attack on the basis of the knowledge of the attacker on the MAC protocol and also on the basis of the ability of the attacker to overpass the different protocols for the authentication and encryption. Four different MAC protocols are considered for calculating the impact of attack on the network as Sensor MAC (SMAC), Timeout MAC (T-MAC), Berkeley MAC (B-MAC), and Gateway MAC (G-MAC). Implementations of selected attacks on MAC, T-MAC, and B-MAC are described and analyzed in detail to validate their effectiveness and analyze their efficiency. As the node in the case of the S-MAC is in sleep mode for 99% of its lifecycle and the attack can make it out of its sleep mode for 100%. Attacks on T-MAC can keep victims awake 100% of the time while the attacker sleeps 92% of the time. With knowledge of protocol because of differences exist in packet structure and timing between WSN MAC protocols, and even without ability to penetrate encryption; all wireless sensor network MAC protocols are susceptible to a full domination attack, which reduces the network lifetime to the minimum possible by maximizing the power consumption of the nodes' radio subsystem. Raymond D. R. et al. [10] has presented the lightweight intrusion detection technique which is based on the host, and so as to resist the node from the denial of sleep attacks the Clustered Adaptive Rate Limiting (CARL) is being described by the author. The limitation of the intrusion detection technique is that it fails to synchronize for the time period when the nodes are not in sleep mode.

So if a node has packet to send, there is no guarantee that other nodes will poll at proper time to overhear a portion of preamble and remain awake for the data packet. The latency is increased by the technique used in the B-MAC in the case of networks with multi hop and in the case when high rate of traffic is being generated then it is being controlled by rate limiting policy. When the rate of packet sending is as mush that it can be considered as the attack then the network traffic is restricted as per the adaptive rate limiting. It can be used to maintain network lifetimes and better throughput at a time even in face of sleep deprivation attack.

Chen C. et al. [11] presented a technique which employs the fake schedule switch having the RSSI measurement aid. The previous attacks are being considered and fake schedule are introduced. Using the above described protocol the node can reduce the harmful effect of the attack and make the attacker to exhaust the energy and even can go upto the state of dead. On the basis of the simulation results it can be stated that the methodology outperforms the other protocols in terms of the bit price, delays, reduction in the packet drop. S-MAC protocol is being considered in the methodology with the duty cycle 10%. In the cases when the packet loss is not caused due to the attacks then the fake schedule is harmful. RSSI is being used in the methodology for assigning values to the nodes and larger value is being assigned to the node that is one hope away from the attacker. Tapalina Bhattasali et al. [12] presented a methodology as a hierarchical framework which is based on the mechanism of distribution collaboration which is generally used for the detection of the sleep deprivation torture in wireless communication network. In heterogeneous sensor field, sensor nodes are categorized into various roles such as sink gateway (SG), sector monitor(SM), Sector-in –charge (SIC) and leaf node (LN) depending on their battery capacity. Where each node has unique responsibility as leaf nodes are used for data sensing, data collection is being done by SIC and the access to the network is being given by the sink gateway.
Ning et al. [13] presented a technique considering the dynamic sleep time instead of going for fixed sleep time in which the energy consumption is minimized ion the case of the sleep state. Global optimal solution is reached using the dynamic programming instead of the differential equations. As dynamic programming is being used for optimal solution and hence using same the optimal solution can be reached in some of the cases and hence for rest the differential equations are being used which are quite hard and complex for implementation.

Fang-Jing wu et al. [14] presented a methodology termed as wake-up scheduling scheme works for collecting data in the wireless network and using the same and works for the energy conservation and for the low reporting latency. In a multi hop wireless network, a simple and efficient way of defining interference neighbors is to prohibit a node from using the same slot0code as those of its 1-hop and 2-hop neighbors. Power saving and latency are improved to prolong network lifetime and freshness of data. Xiaoming et al. [7] presented a methodology which is based on the threshold defense scheme and reduces the effect of different synchronization attacks. A threshold clock drift is being defined and the SYNC messages whose relative time for sleep is larger than the threshold are ignored. As the result of ignorance the connection between two nodes may be temporarily banned just to prevent propagation of the attack. This strategy penalizes abnormal large clock drifts and sacrifices local communication to save global stability.

C.C. Li. Et al. [16] presented a methodology for the exhaust of energy attacks. So as to perform the energy exhaust attacks the attacking node should have the information about the victim node. For the purpose of the counteraction the author have used the fake schedule scheme. Because of the collision attacks the receiver fails to receive the same number packets as the node have send the CTS to the other nodes. As the receiver doesn't receive the packets then the sender will not get the ACK packet from the receiver side. Namely, the victims and all their neighbors broadcast schedule switch SYNC but do not really change their schedule. And after a timer Timeout Back expires, they all come back to their former schedule and synchronization. Rainer Falk et al. [17] presented a methodology as wake up scheme in which the sensor nodes can be in active state from the sleep mode after receiving the wake up token. Different limitations of IEEE 802.15.4 are being addressed in the methodology so as to prevent the node from the denial of sleep attacks. The sensor nodes are in ready state when the node receives the wake up radio from the nodes which are legitimate and are authenticated. Jingjun et al. [18] presented a methodology for the hierarchical wireless sensor networks for the system security and the ways for detecting the denial of service are discussed and the harmful intruders are being tracked. An Artificial Immune System (AIS) approach and multiple-target tracking techniques are adopted to detect security threats in WSNs. To prevent WSN from sleep deprivation attacks, authentication-based counter-measures are proposed in [19] for three topology maintenance protocols (PEAS, CCP, and ASCENT). The message authentication codes are computed using the pair wise shared keys are then transferred to different neighboring nodes for the purpose of the authentication. All type of intruder attacks are then avoided using the authentication of the nodes for all types of communication.

V. CONCLUSION

In this paper certain type of attacks in WSN and the different methodology for the prevention of the attacks are discussed. From the study of the different methodologies for the prevention of the attacks discussed above the power of a sensor node(s) and security in WSN is essential as it helps in determining how probable a network is used for further transmission. And it helps in increasing the overall life and accuracy of the network.

REFERENCES

1. D. Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4," IETF RFC 4728, vol. 15, pp. 153-181, Feb. 2007.
2. C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On-Demand Distance Vector (AODV) Routing," IETF RFC 3561, July 2003.
3. E. M. Royer, C.Toh, "Review of current routing protocols for ad hoc mobile wireless networks", IEEE Personal Communications, 6(2), pp. 46-55, 1999.
4. F. Wu and Y. Tseng, "Distributed Wake-up scheduling for Data collection in tree-based wireless sensor networks," IEEE Communications letters, Vol. 13, No.11, November 2009.
5. F. Stajano, R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks," In ICISC, Springer-Verlag, 2000.
6. M. Pirretti, S. Zhu, N. Vijaykrishnan, P. Mcdaniel, and M. Kandemir, "The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense," International Journal of Distributed Sensor Networks, pp.267–287, 2006.
7. L. Xiaoming, M. Spear, K. Levitt, N.S. Matloff, and S.F. Wu, "A Synchronization Attack and Defense in Energy-Efficient Listen-Sleep Slotted MAC Protocols," SECURWARE '08. Second International Conference on Emerging Security Information, Systems and Technologies, pp. 403-411, 2008.
8. M. Brownfield, Y. Gupta, Mem and N. Davis IV, "Wireless Sensor Network Denial of sleep attack," IEEE 2005.
9. D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midkiff, "Effect of Denial of sleep attacks on wireless sensor network MAC protocols" published by IEEE 2008.
10. D.R. Raymond and S. F. Midkiff , "Clustered Adaptive Rate Limiting: Defeating Denial-Of-Sleep Attacks In Wireless Sensor Networks," Military Communications Conference, 2007, MILCOM 2007, IEEE, pp. 1-7.
11. C. Chen, L.Hui, Q.Pei, L. Ning, P. Qingquan, "An Effective Scheme for Defending Denial-of-Sleep Attack in Wireless Sensor Networks," Proceedings of the 2009 Fifth International Conference on Information Assurance and Security, Vol. 02, IEEE CS, 2009.
12. T. Bhattasali, R. Chaki, S. sanyal, "Sleep deprivation Attack Detection in Wireless Sensor network", International Journal of Computer Applications, February 2012.
13. X. Ning and C. G. Cassandras, "Optimal Dynamic Sleep Time Control in Wireless Sensor Networks," IEEE Conference on Decision and Control Cancun, Mexico, Dec. 9-11, 2008.
14. F. Wu and Y. Tseng, "Distributed Wake-up scheduling for Data collection in tree-based wireless sensor networks" published by IEEE Communications letters, Vol. 13, No.11, November 2009.
15. M. Stahlberg, "Radio Jamming attacks against two popular mobile networks," In Helsinki University of Tech. Seminar on Network Security, 2000.
16. C.C. Li, H.Q. Pei, and L. P. Ning, Qingquan, "An Effective Scheme for Defending Denial-of-Sleep Attack in Wireless Sensor Networks," Fifth International Conference on Information Assurance and Security. pp. 446-449. 2009.
17. F. Rainer, and H. Hans-Joachim, "Fighting Insomnia: A Secure Wake-Up Scheme for Wireless Sensor Networks," Third International Conference on Emerging Security Information, Systems and Technologies, pp.191-196, 2009.
18. J. Zhao, and K.E. Nygard, "A Two-Phase Security Algorithm for Hierarchical Sensor Networks," FUTURE COMPUTING 2011: The Third International Conference on Future Computational Technologies and Applications, pp. 144-120. 2011.
19. A. Gabrielli, L.V. Mancini, S. Setia, and S. Jajodia, "Securing Topology Maintenance Protocols for Sensor Networks: Attacks and Countermeasures," IEEE Transactions on Dependable and Secure Computing, pp. 450 – 465, 2011.

