ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Performance Analysis of Cluster Based Protocols in Sensor Networks and their Vulnerabilities

Andhe Dharani[1], Manjuprasad B[2], Shantharam Nayak[3], Vijayalakshmi M.N[4]

Professor, Dept of MCA, R.V. College of Engineering, Mysuru Road, Bengaluru, Karnataka, India

Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India[1]

VTU Research Scholar, Dept of ISE Research Centre, R.V. College of Engineering, Mysuru Road, Bengaluru, Karnataka, India

Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India[2]

Professor, Dept of ISE Research Centre, R.V. College of Engineering, Mysuru Road, Bengaluru, Karnataka, India

Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India[3]

Associate Professor, Dept of MCA, R.V. College of Engineering, Mysuru Road, Bengaluru, Karnataka, India

Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India[4]

ABSTRACT: Wireless sensor networks as gained lots of impact in the real time applications like monitoring, surveillances and tracking. These applications are mainly rely on the collection of critical information where manual information collection is very difficult task. WSNs are more vulnerable to many types of threats, providing security will be very complex due to the resource constraint sensors. The proposed work aims to study and analyze the vulnerabilities and its effect on the performance of sensor networks in cluster based routing protocols. An exhaustive analysis is presented by captivating the standard clustering architecture with its different stage of operating modes. A comparison is done for with latest existing security solutions which mainly deal with cluster based protocols in wireless sensor networks. An Open Systems Interconnection layer wise comparison is presented with the possible vulnerabilities at each layer. This work also enlightens the literal need of security and its requirements in wireless sensor networks for an efficient information system.

KEYWORDS: Vulnerability; Threats; Security Requirements; Security Challenges; Clustering; Confidentiality; Integrity; Authentication; Data freshness;

I. INTRODUCTION

God has created humans with five sensors, but humans are created more than 50 basic sensors which can sense parameters like, odour, taste, electric charges and many. As trends in sensor technology is emerging, its applications also gaining lots of impact in real world. Wireless sensor networks (WSNs) are one of the most prominent communication technology built over these sensors. WSNs are the networks of limited resource nodes with some wireless link. These nodes are deployed in human unattended areas where collection of information is very necessary and difficult [1] [2]. Due to its wireless nature which operates on low frequency channel it is more vulnerable to wide range of attacks. The major security requirements in wireless sensor networks are confidentiality, integrity, authentication and availability. The attacks on the these networks can be from inside or outside where inside attacks is due to malfunctioning of the original nodes and outside attacker [3][4]s are due to deployment a malicious nodes[5] which can easily communicate with other types of nodes.

10.15680/ijircce.2015.0304107

Security in WSNs has gained lots of important in recent WSNs research [6]. Many researchers had contributed ideas in proposing solutions and effective defences against many attacks [7-13]. WSNs has a wide range of applications in the future while contributing in the field of Internet of Things and Big Data for many real time application[14] and data analysis for many social and security applications.

1.1. Need of Security in WSNs[15]: As the major application so these WSNs is collection of information during monitoring environmental changes and battle field surveillance, but security in necessary only in some critical applications.

Security in battle field surveillance in very crucial as the attacker can malfunction the internal node and can also deploy the malicious nodes. These operations may lead to loss of critical information by Intercepting, Modifying and fabricating the message sent by original nodes [16]. In some applications the attackers may try only to destroy the monitoring system without concentration on the message by tampering the nodes or by attacking on the physical layer of the nodes.

1.2. Security Challenges: There are many hindrance and constraints involved when designing a security protocol for WSNs. The limited memory, storage, processor capabilities and harsh environmental conditions may restrict the researchers for providing security protocols. The summarization of the security challenges in sensor networks from some research article [7][17][18] is as follows:

- Providing the necessary security requirements by minimizing the resource consumption of the nodes
- Concentrating on the security solutions suitable for particular types of applications
- Aiming to maintain the performance of the developed security protocols
-

II. RELATED WORK

This section focuses on analyzing the performance and vulnerability of the clustering protocols. First a discussion of clustering is made for studying the working mechanism of the clustering in WSNs [19].

2.1. Clustering Protocols: This is promising protocol which can be used for efficient information transfer in WSNs[20], this include data aggregation, distributed data collection, hop by hop message transfer. These factors made the clustering protocol to use the resources of the nodes very efficiently and increase the lifetime of the networks. Currently there exists many clustering protocol which operates on different factors as discussed bellow.

2.1.1. Operation Modes of Clustering: All the clustering protocols are mainly operated on 2 phases, setup phase and steady phase. Many researchers have proposed different way of phase operation; some of them are discussed here.

2.1.2. Different Setup phases: In this phase there will be formation of cluster head and cluster through advertizing. The node which is selected as cluster head will broadcast the message to its surrounding nodes for joining its cluster, based on the signal strength the node will decide to become its member. There are various criteria for selecting the cluster head like-random selection, based on high energy, based on the density of nodes. This clustering will reduce the energy consumption of the nodes by avoiding redundant data, reducing communication distance i.e. instead of nodes send their data to base station it can be grouped in-between and transferred to base station via cluster head.

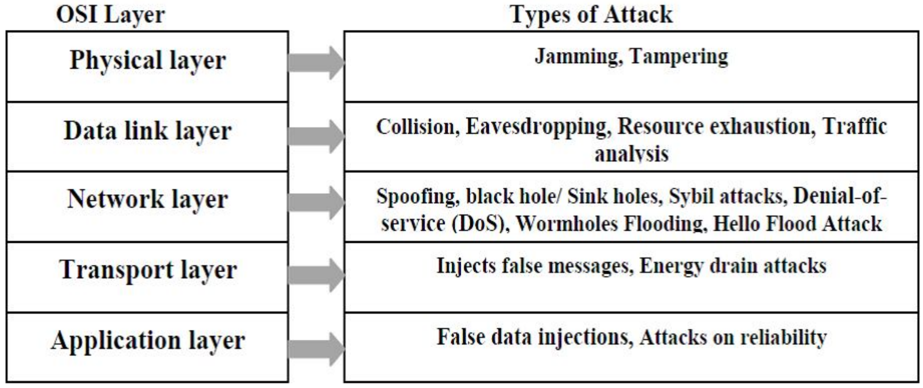
*2.1.3. Different steady **Phase:*** This phase mainly contribute how to transfer the data. This phase includes direct data transfer to base station and indirect data transfer to base station via cluster head. This phase included hop by hop data transfer with an optimum path selection.

Low Energy Adaptive Clustering Hierarchy (LEACH) [21] the most popular cluster based protocol. Based on the LEACH many protocol were proposed by adding additional features and different operation modes like REBCH [22], EECH [23], HEED [24], and QIBEEC [25] were proposed with different way of selecting of cluster head, formation of clusters, data aggregation.

The operating nature of clustering protocol had gained lots f impact in efficient power utilization for increasing the lifetime of the nodes. But it is very vulnerable for many threats as its relay on cluster heads for data aggregation and routing, if the attacker malfunctioned or destroy these heads means there will be no assurance for the originality of the information.

III. VULNERABILITY ANALYSIS IN CLUSTERING PROTOCOLS

One of the major vulnerability [26] in WSNs is due to the deployment of sensors which are scattered in insecure place and the wireless nature makes it more prone to attacks. This section identifies the vulnerabilities and threats in each Open Systems Interconnection (OSI) layer.



OSI Layer	Types of Attack
Physical layer	Jamming, Tampering
Data link layer	Collision, Eavesdropping, Resource exhaustion, Traffic analysis
Network layer	Spoofing, black hole/ Sink holes, Sybil attacks, Denial-of-service (DoS), Wormholes Flooding, Hello Flood Attack
Transport layer	Injects false messages, Energy drain attacks
Application layer	False data injections, Attacks on reliability

Figure.1: Types of Attacks [15]

Figure.1 shows the various attacks on major Open Systems Interconnection (OSI) layers [1] of WSNs these attacks rely on the vulnerabilities at these layers. The following are the vulnerabilities in clustering at major OSI layers.

3.1. Physical Layer Vulnerabilities: Once the cluster head is selected it sends a request to its surrounding for forming a cluster through advertising itself. This advertising may be received by malicious nodes and may create traffic causing interference at the cluster heads. This leads to more power dissipation from the cluster heads and reduce the network lifetime. Another type of attack can be tampering the nodes and make it useless.

3.2. Data Link Layer Vulnerabilities: This layer is the major layer of OSI which is more prone to attacks and there is a need of countermeasures to secure it. The main vulnerability is the broadcast and multicast message transfer; this can affect the confidentiality of the information. The information transmitted from one node can be easily received by others. If the information sent from cluster heads is not kept confidential means the whole system can be insecure as the cluster head have the aggregated information.

3.3. Network Layer and Transport Layer Vulnerabilities: This layer is mainly vulnerable during the data transmission phase. The information transmitted by cluster head may not reach the base station via trusted hop. This may cause the loss of information or delay in the transmissions which make the system halt. This vulnerability may also contribute to more energy dissipation of the cluster head. The intruder may manages to become cluster head which may receives information from the members and send false packets to other hops and base station. However, because it is a cluster based protocol

These vulnerabilities in clustering can be reduced using some of the general counter measure as discussed in [1] using Channel hopping, Blacklisting, CRC, Encryption and Decryption. There are some specific methods which mainly focus on the some of the key concepts as discussed below.

SLEACH [27]: is the first security enhanced implementation over LEACH. This protocol made a analysis on the security issues in cluster based protocols for a resources constraints devices.

Sec-LEACH [28]: This protocol provides an efficient secure clustering by implementing additional features to LEACH for providing cluster based security. This protocol uses a random-key distribution with a fixed pool of key and µTESLA for hierarchical clustering in WSNs with dynamic cluster formation. Based on this key distribution it tries to identify the malicious nodes.

FLEACH [29]: Provides a secured peer to peer information transfer in LEACH based protocol by using a random key per-distribution with symmetric key cryptography to improve the security features in cluster based protocol.

3.4. Novel Approach for Secured Communication in WSN Using Dynamic Low-Weight Keys [NPSC] [30]: A hierarchical protocol based on LEACH for heterogeneous networks is proposed in [30], using a dynamic low weight keys. A pair of keys is assigned to each pair of the nodes called two way keys. In associated a cluster head will use the common key to communicate with bases station with a manufacturing code. This protocol made some assumption like Base station has no resource constraints; network is heterogeneous where high security nodes are used as trusted nodes which can also withstand tampering attacks. A unique code called Manufacturing Code and a Hash code is used as the private key of length 64 bits. This protocol is designed to withstand the 4 threats i.e. Threat0, Threat1, Threat2 and Threat3 caused by the malicious nodes.

- Threat0 malicious node can be restricted using time validation process of hello packets.
- Threat1 can be prevented using the allocation time of the cluster head.
- Threat2 is prevented using the above 2 process with a secret key matching techniques
- Threat3 node is restricted using all 3 processes with hash code of the particular node with base station.

3.5. CIAWSNs protocol for Secure Information Transmission [31]: A light weight key without distribution techniques is proposed in our previous work [31] called as CIAWSNs, focused on providing a simple low complex secure mechanism for resource constrained WSNs. Using this on the basic security requirements of the WSNs is achieved with an optimal resource usage. This protocol also has some security level assumptions. It assumes that during initial deployment there will be no malicious nodes in the network. Some numbers of malicious nodes are used for create attacks in the networks. These malicious nodes are functioned only to send the false information, packet sniffing and to make hello attack. This protocol operates only on some set of firewall rules, device identification and key compression at the cluster head for maintaining data confidentiality.

This protocol is resistance to the following attacks:

- Eavesdropping: Ensuring confidentiality of the information in WSNs
- Packet Sniffing: Ensuring integrity of the message transferred from cluster heads
- False Message: Ensuring authentication of the message that it is from genuine source.

Comparisons between the protocols were made to analyse the energy utilization by the nodes in the network while achieving security requirements. Figure-2 shows the lifetime of the network where the ***NPSC*** [30] is compared with LEACH which is simulated for 100 numbers of nodes for 800 rounds. The NPSC[30] has implement a secure cryptographic techniques, as a result the protocol is secure but the number of failure nodes is more compared to LEACH which is without security.

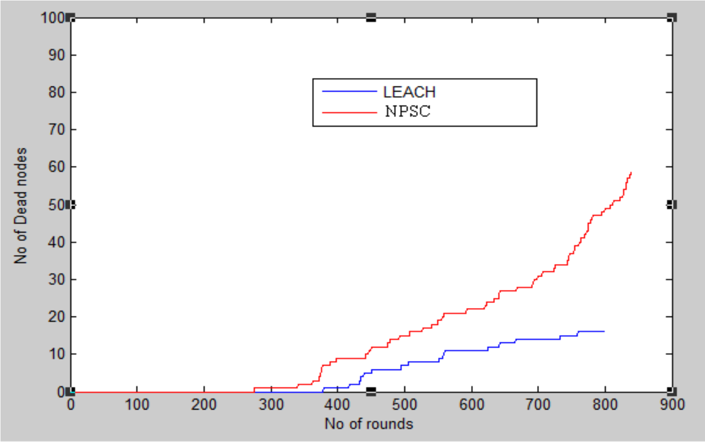


Figure-2: Network Lifetime [30]

Figure-3 shows the lifetime of the CIAWSNs which is also a based on LEACH protocol which is simulated with 100 number of nodes for 800 rounds. This protocol aims to provide security with low complex solutions by using firewall, device identification and key compression. The life time of the nodes is last is 39% where is in figure-2[30] it is 60%. The first node dead is before 300th rounds in figure-2 but in CIAWSNs the first node dead is at around 350th rounds. Using this [31] light weight secure solution the lifetime of the network is increased by 21% compared to [30].

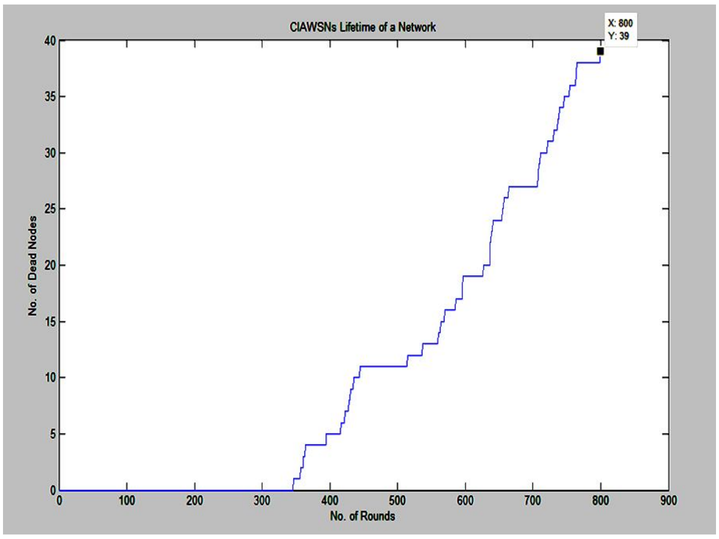


Figure-3: Network Lifetime

This concludes that using light weight security solution one can improve the performance of WSNs over existing cluster based protocols. Even though in the recent years energy is not a constraints due to harvesting of energy using environmental conditions, but it can reduce the complexity at the node side.

IV. Conclusion and Future Work

This work aims to analyse the vulnerabilities and security requirements necessary for secure information transfer in Wireless Sensor Networks. These analyses are produced for identifying the vulnerabilities at major Open Source Interconnection (OSI) layers of WSNs with the associated threats. This work mainly focused on analysing the security performance of cluster based protocols with efficient resource utilization. This shows that how secure is the clustering protocols and how it can be enhance for achieving more security requirements. The standard secure cluster based protocols are discussed with their advantages and it is compared with each other for better analysis by considering its vulnerabilities. Clustering is one of the best routing protocols in WSNs; hence this work focused to enhance the feature of clustering by identifying its vulnerabilities in providing security for efficient information transfer. The future work of this work can be an implementation of an enhanced secure protocol of CIAWSNs for heterogeneous WSNs by incorporating the analysis done.

REFERENCES

1. Hemanta Kumar Kalita and Avijit Kar, M, “Wireless Sensor Network Security Analysis,” *International Journal of Next-Generation Networks (IJNGN)*,Vol.1, No.1, December 2009.
2. D. Boyle, T. Newe, ”Securing Wireless Sensor Networks: Security Architectures”, *Journal of Networks*, 2008, 3 (1).
3. X. Du, H. Chen, "Security in Wireless Sensor Networks", *IEEE Wireless Communications*, 2008.
4. J. Granjal, R. Silva, J. Silva, "Security in Wireless Sensor Networks", *CISUC UC*, 2008.
5. Y. Zou, K. Chakrabarty, "Sensor deployment and target localization based on virtual forces", *INFOCOM 2003. Twenty- Second Joint Conferences of the IEEE Computer and Communications Societies IEEE*, Volume: 2, Pages: 1293 - 1303, April 2003.
6. Wenjun Gu, Xun Wang, Sriram Chellappan, Dong Xuan and Ten H. Lai,” Defending against Search-based Physical Attacks in Sensor Networks”, Department of Computer Science and Engineering, The Ohio State University, Columbus, OH 43210, U.S.A.
7. A.Perrig, J.Stankovic, and W.David, “Security in wireless sensor networks,*” in Communications of the ACM*, Vol 47, No. 6, pp. 53-75, 2004.
8. C. Karlof and D. Wagner, ”Secure routing in wireless sensor networks: Attacks and countermeasures,” *in Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications (WSNA)*, May 2003.
9. A.D.Wood and J.A.Stankovic,”Denial of service in sensor networks ,*in IEEE Computer*, pp. 54-62, 2002.
10. A.Perrig, R.Szewczyk, J.D.Tygar, V.Wen, and D.E.Culler,”Spins: Security protocols for sensor networks,*” in Proceedings of the 7th Annual International Conference on Mobile Computing and Networking(MobiCo*m), July 2001.
11. John R. Douceur, “The sybil attack, in *Proceedings of the 1st International Workshop on Peer-to-Peer Systems*, March 2002.
12. J.Newsome, E.Shi, D.Song, and A.Perrig,”The sybil attack in sensor networks: Analysis and defenses,” in *Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks(IPSN)*, April 2004.
13. Y.C.Hu, A.Perrig, and D.B.Johnson, “Packet leashes: A defense against wormhole attacks in wireless ad hod networks, in *Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, April 2003.
14. Verena Weber, It contributed to the “ICTs, ”The environment and climate change”, *OECD Conference* at Helsingør, Denmark, May 2009
15. Manjuprasad B, Andhe Dharani,” Necessitate for Security in Wireless Sensor Network and its Challenges”, *International Journal of Research in Computer Applications & Information Technology*, ISSN Online: 2347- 5099, Volume 1, Issue 1, pp. 21-25, July-September, 2013
16. Anil M. Hingmire, “Enhancing Security of Wireless Sensor Network”, *International Journal of Engineering Science and Innovative Technology (IJESIT)* ISSN: 2319-5967 Volume 2, Issue 2, March 2013.
17. Granjal, Jorge, Edmundo Monteiro, and Jorge Sá Silva. "Security in the integration of low-power Wireless Sensor Networks with the Internet: A survey." Ad Hoc Networks 24, pp. 264-287, 2015
18. Mahmood, Muhammad Adeel, Winston KG Seah, and Ian Welch. "Reliability in Wireless Sensor Networks: A Survey and Challenges Ahead." Computer Networks, 2015.
19. Andhe Dharani, Vijayalakshmi M.N, Manjuprasad B, “An Epigrammatic Study of some of the Fundamental Concepts in Wireless Sensor Networks”, *International Journal of Emerging Technology and Advanced Engineering*, ISSN 2250-2459,Volume 2, Issue 9, pp.424-428 September 2012.
20. Andhe Dharani, Vijayalakshmi M.N, Vijay Singh, Sumithra Devi K.A “Power Optimization in Adhoc Sensor Networks using Clustering Approach”, *Proceedings of the World Congress on Engineering*,ISSN:2708-0958(Print); ISSN:2708-0966(Online), 2011
21. W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan.” Energy Efficient Communication Protocol For Wireless Micro sensor Networks”,. *In Proceedings of the Hawaii International Conference on System Sciences*, January 2000.
22. Manjuprasad B, Andhe Dharani, Vijayalakshmi, “Residual Energy Based Clustering Algorithm for Mobile Nodes in Sensor Networks”, *International Journal of Computer Networking, Wireless and Mobile Communications IJCNWMC)* ISSN 2250-1568Vol. 3, Issue 1, pp 281-288, 2013
23. Seema Bandyopadhyay and Edward J. Coyle,” An Energy Efficient hierarchical Clustering Algorithm for Wireless Sensor Networks”, *School of Electrical and Computer Engineering , Purdue University West Lafayette*, IN, USA.
24. Ossama Younis and Sonia Fahmy,“ Distributed Clustering in Ad-hoc Sensor Networks:A Hybrid, Energy-Efficient Approach,” *Department of Computer Sciences, Purdue University, 250 N. University Street*, West Lafayette, IN 47907–2066, USA
25. Manju Prasad, Andhe Dharani, “A QoI Based Energy Efficient Clustering for Dense Wireless Sensor Networks”, International Journal Of Advanced Smart Sensor Network Systems (IJASSN), ISSN 2231- 4482, Vol 3, No.2, pp.1-9, April 2013.
26. S. Mohan , S. Grace Diana . S. Ramya, “A Survey on Wireless Sensor Network Security”, International Journal of Innovative Research in Computer and Communication Engineering”, Vol.2, Special Issue 1,pp.1100-1104,2014
27. Mohamed-Lamine Messai, “Classification of Attacks in Wireless Sensor Networks”, *International Congress on Telecommunication and Application*-14, University of A.MIRA Bejaia, Algeria, APRIL 2014
28. Oliveira L. B. et.al, “Secleach - a random key distribution solution for securing clustered sensor networks”. *In Proc. of the Fifth IEEE International Symposium on Network Computing and Applications*, pages 145–154, Washington, DC, USA, 2006..
29. A. C. Ferreira, M. A. Vilaca, L. B. Oliveira, E. Habib, H. C. Wong, and A. A. Loureiro, “On the security of cluster-based communication protocols for wireless sensor networks,” in Proceedings of the 4th IEEE International Conference on on Networking, pp. 449–458, 2005.
30. Urmila Devi,” A Novel Approach for Secured Communication in WSN Using Dynamic Low-Weight Keys”, *International Journal of Computer Science and Information Technologies*”, (IJCSIT), Vol. 4 (4) , pp.619-624, 2013.
31. Manjuprasad B, Andhe Dharani, Shantharam Nayak, ” An Energy Efficient Packet Filtering system in Sensor Networks,” American Journal of Sensor Technology, ISSN (Online):2373-3462, Vol. 2, Issue-3, pp.34-39, 2014

BIOGRAPHY

Dr. Andhe Dharani is a Professor, in the Department of Master of Computer Application, R.V. College of Engineering, Bengaluru. She has completed a project funded by NRB, DRDO, India. Her research interests are Image Processing, Wireless Sensor Networks, and Big Data Analytics. She has published many research articles in International Journal, IEEE International Conferences and a book on Wireless Sensor Network.

Mr. Manjuprasad B is a Research Scholar, pursuing Ph.D. under Visvesvaraya Technological University, Belagavi. He completed is B.E in 2011 from VTU and worked as Research Fellow for the project funded by NRB, DRDO, India. His research areas are Wireless Sensor Networks, Big Data.

Dr. Shantharam Nayak is a Professor, in the Department of Information Science and Engineering, R.V. College of Engineering, Bengaluru. He is a senior member of Computer Society of India, serving CSI since 1996 in its activities. He has published many research articles in various Journals and Conferences. His research interests are Software Engineering, Software Performance, and Operating Systems.

Dr. Vijayalakshmi M.N is an Associate Professor, in the Department of Master of Computer Application, R.V. College of Engineering, Bengaluru. She has published many research articles in International Journals, IEEE International Conferences and a book on Wireless Sensor Network. Her current research interest includes Data mining, Image Processing, Computer Vision and Wireless Sensor Networks.