International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 3.45 (SJIF-2015), e-ISSN: 2455-2585
Volume 4, Issue 5, May-2018

Effect of Various Networks Security Attacks on WSN Based upon Residual Energy

Pankaj Chandra[1], Santosh Soni[2]
[1]Information Technology, SoS-Engineering & Technology, Guru Ghasidas Vishwavidyalay, Bilaspur, Chhattisgarh, India
[2]Information Technology, SoS-Engineering & Technology, Guru Ghasidas Vishwavidyalay, Bilaspur, Chhattisgarh, India
E-mail[1]: pankaj2684@gmail.com, E-mail2: santoshsoni.77@gmail.com

Abstract*: *Wireless Sensor Networks are widely used in data gathering and data transmission with the help of wireless networks. Now a day's various researchers are determining the location of nodes by Wireless Sensor Network localization algorithms, which have been proved as a boon to the research study. The sensor nodes are Week to most of security attacks like Wormhole attack, Sybil attack, spoofing attack, replay attack, due to the weakness in WSN, which degrade their performance. In this research paper we have tested Wireless Sensor Network localization algorithms by mobility of sensor nodes and size of packets as performance matrices, to find out the compromised WSN nodes residual energy. The simulation result shows the vulnerability to network security attacks.

Key words: WSN Localization Algorithm, Wireless Sensor Network

I-INTRODUCTION

Wireless sensor networks are consisting of large number of sensor nodes that interact with environment with the help of sensors. Wireless sensor network has become popular due to its applications in many different areas, such as medical, industrial, defense and environmental. Wireless sensor networks are used in data gathering and data transmission with the help of wireless networks. One of the main challenges in Wireless sensor network is security. Several physical properties can be monitored by a Wireless sensor networks: humidity, light, temperature and movements. Usually the collected information and sensor nodes must be localized in space to identify the location of event. The positioning is achieved using a localization system. Localization systems are a key part of Wireless sensor networks. Due to their key role on Wireless sensor networks localization systems can be a target of an attack that could compromise the entire functioning of a Wireless sensor network. In this paper we have shown that current localization systems are Week to these security attacks. The impact of network security attacks finally reduces the residual energy of wireless sensor networks node. The various sanction of this research study is as follows –

Section I - Introduction	Section IV - Network Security Attacks
Section II - Previous Work	Section V - Simulation Setup and Results
Section III - WSN Localization Algorithms	Section VI - Conclusion

II-PREVIOUS WORK

Various localization algorithms have been proposed for research outcome based upon certain performance matrices.

[I] Nick et al. [1] has provided a comprehensive review and comparison of recent implementations of physical measurement techniques used in sensor localization, and of the localization algorithms that apply these measurement techniques.

[II] Asma Mesmoudi , Mohammed Feham and Nabila Labraoui [3] compared the most relevant localization algorithms and discuss the future research directions for wireless sensor networks localization schemes.

[III] Svarika Goyal, Tarunpreet Bhatia , A.K. Verma [5], In this paper, various types of attacks have been studied and defensive techniques of one of the severe attacks i.e. wormhole and Sybil are surveyed in major detail with the comparison of merits and demerits of several techniques.

[IV] Xu et al. [8] described different cryptographic methods can be used to defend against some such attacks. But the inside attacks are not detectable with only the classic cryptographic techniques.

[V] Ismail and Chia Chin [11] present numerous localization algorithms with different accuracies, computational complexities, a-priori knowledge requirements with different levels of robustness.

[VI] Boukerche et al. [16] presents a localization system under various network security attacks with various security techniques.

[VII] S. H. Hong, B. K. Kim and D. S. Eom [18] present various localization algorithms with network mobility.

III- WSN LOCALIZATION ALGORITHMS

Many localization algorithms for Wireless Sensor Networks exist today. Some Examples are MCL, KALMAN, IMCL, SMPL and MPL. All the localization systems require an infrastructure setup, which provide important location information of sensors and event occurrences. All the current localization systems for Wireless Sensor Networks are two step processes as explained below.

A.1 Distance or Range Estimation

Distance or range estimation is used to finding the distances between the nodes using any one of the many existing ranging techniques like Timing based (TOA, TDOA), Directionality based (AOA), Signal strength based (RSSI), and Hop based (DV-HOP, Hop TERRAIN).

A.2 Position or Location Computation

Position or Location Computation step involves calculating the position of a node relative to a fixed coordinate system

B. Classification scheme for Localization System

Using the Distance estimation, we classify the localization algorithms as range based and range free localization algorithms. Range based systems, uses Timing based (TOA, TDOA), Directionality based (AOA), or Signal strength based (RSSI) for distance estimation and position of sensor nodes are computed using triangulation or multilateration. Range free localization algorithms uses Hop based (DV-HOP, Hop TERRAIN) techniques for distance estimation and finding the position of sensor nodes.

IV-NETWORK SECURITY ATTACKS

Many attacks which generally shows the distance and position computations in very common attacks in existing localized systems. The parts of a localization system, develops the various type of vulnerabilities jointed with various systems, as it is in multihop algorithm. These attacks mainly includes Sybil, Replay, Wormhole and Duplicate attack [01][11][12][13][15].

Sybil Attack: That contains various set of different node and continues sending wrong information.
Replay Attack: This is the clone of the initial packet, The neighboring nodes wrongly deduct that the infected node is the node which has sent out the initial packet. [01][11][12][13][15].
Wormhole Attack: That contains the information submitted by any infected node is forwarded to other side of the network and made the clone by any specific infected node on the other side of the network. [01][11][12][13][15]
Compromise Attack: These nodes contain minimum three stages: generally obtaining with compromising the sensors. [16][17].

V- SIMULATION SETUP AND RESULT

To Test the Wireless Sensor Network localization algorithms by mobility of sensor nodes and size of packets as performance matrices, it is simulated in a dot net framework based WSN Localization Simulator. WSN Localization Simulator supports completely large scale networks. The used WSN localization simulation tool is based upon two main software layers, a core simulator layer and a localization layer. Here, Table 01 containing various WSN Localization Simulation parameters information:

Table 01: Simulation Setup

Simulator	WSN Localization Simulator
WSN Localization Algorithms	Kalman, Monte Carlo , Improve Monte Carlo, Mobility Prediction Localization , Secure MPL
Network Security Attacks	Wormhole, Sybil, Compromise and Replay
Mobility of WSN Nodes	10 , 20 and 30 m/sec
Packet Size	256 , 512 and 1024 Bytes
Temperature	25 Degree
WSN Node Density	50
Sensor's Mobility Model	Modified Random Waypoint
Anchor's Mobility Model	Modified Random Waypoint
Number of Anchor Nodes	150
Sensor Model	Mica2
Propagation Model	Two-Ray Ground
Simulation Time	150 Seconds

5.1 Simulation Results

In this research paper we have tested Wireless Sensor Network localization algorithms by mobility of sensor nodes and size of packets as performance matrices, to find out the compromised WSN nodes residual energy. The Figures [01 -06] and Tables [02-03] are showing the performance of localization algorithms in form of WSN node's residual energy against various network security attacks.

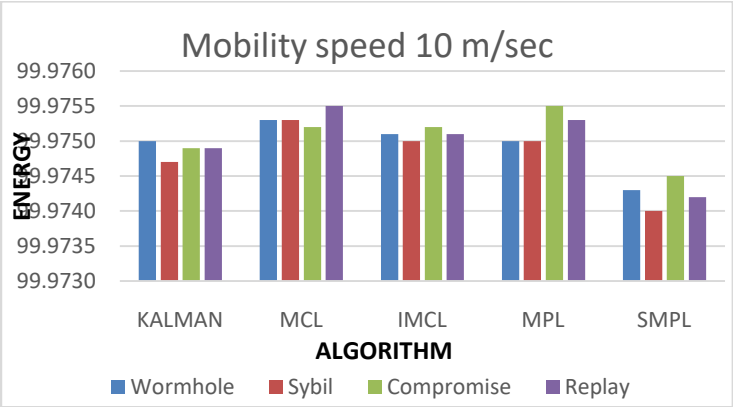

Figure 01: Performance of WSN Localization Algorithms vs Network Security Attacks under Mobility Speed 10 M/Sec

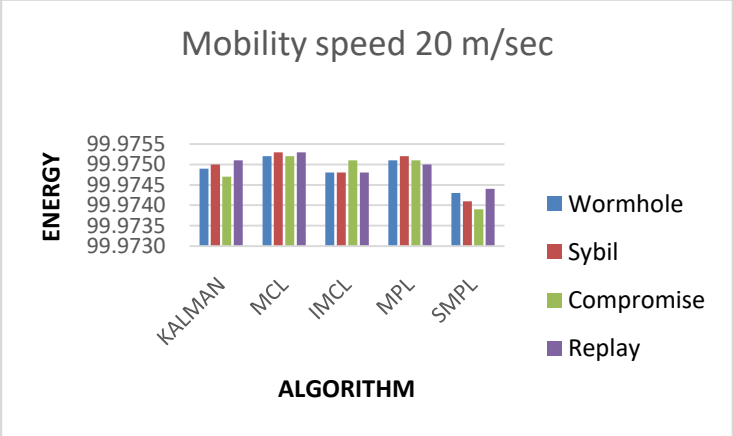

Figure 02: Performance of WSN Localization Algorithms vs Network Security Attacks under Mobility Speed 20 M/S

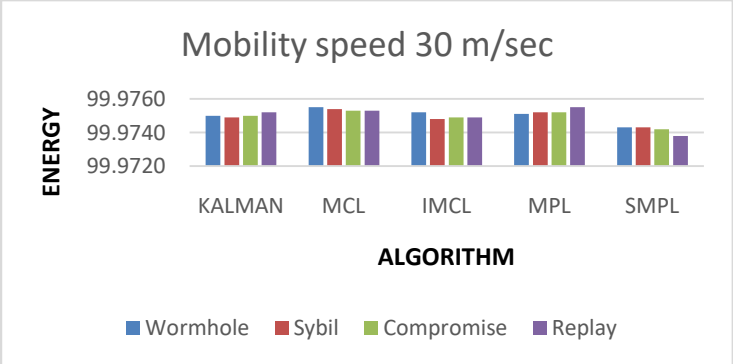

Figure 03: Performance of WSN Localization Algorithms vs Network Security Attacks under Mobility Speed 30 M/S

	Wormhole	Sybil	Compromise	Replay
1.Kalman	Week	Week	Not Week	Not Week
2.MCL	Week	Not Week	Not Week	Not Week
3.IMCL	Not Week	Not Week	Not Week	Week
4.MPL	Not Week	Week	Week	Not Week
5.SMPL	Not Week	Week	Not Week	Week

Table 02: Vulnerability of WSN Localization Algorithm against Various Network Security Attacks under the performance matrices of Mobility of WSN Nodes

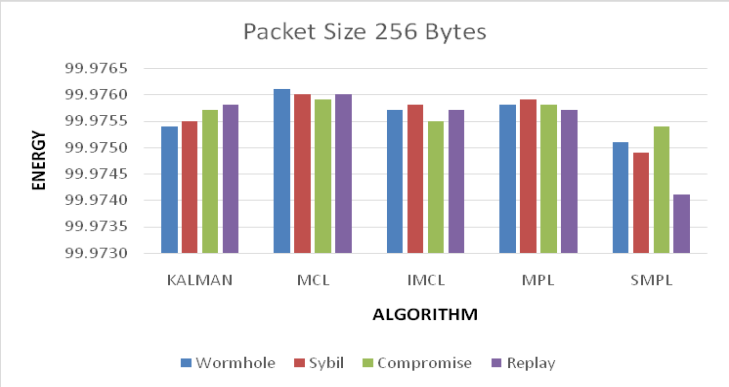

Figure 04: Performance of WSN Localization Algorithms vs Network Security Attacks under Packet Size 256 Bytes

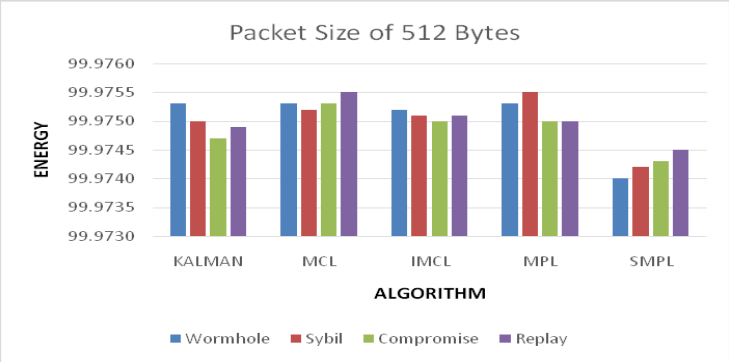

Figure 05: Performance of WSN Localization Algorithms vs Network Security Attacks under Packet Size 512 Bytes

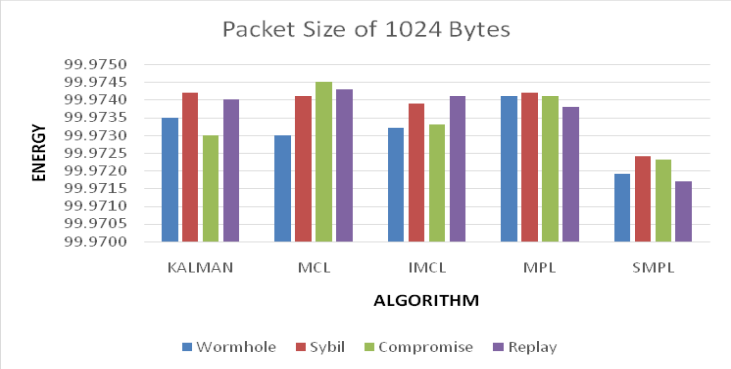

Figure 06: Performance of WSN Localization Algorithms vs Network Security Attacks under Packet Size 1024 Bytes

	Wormhole	Sybil	Compromise	Replay
1.Kalman	Week	Week	Not Week	Week
2.MCL	Week	Not Week	Week	Not Week
3.IMCL	Week	Not Week	Week	Week
4.MPL	Not Week	Week	Not Week	Not Week
5.SMPL	Not Week	Week	Week	Week

Table 03: Vulnerability of WSN Localization Algorithm against Various Network Security Attacks under the performance matrices of packet size of WSN Nodes

IV-CONCLUSIONS

Localization algorithms provide fundamental support for different location aware protocols. In this paper we have investigated localization algorithms with respect to mobility of sensor nodes and size of packets as performance matrices. This research study has shown that the sensor nodes are Week to most of security attacks, which is summarized in Table 02 and Table 03. MCL, IMCL and SMPL algorithms shows good performance against Sybil attack.

References

[1] Nick Iliev, Igor Paprotny, Review and Comparison of Spatial Localization Methods for Low Power Wireless Sensor Networks, Submitted To The IEEE Sensors Journal, Vol. 15, Issue 10, PP. 5971-5987, (2015)

[2] L. Chen et al.,Distributed range-free localization algorithm for Wireless Sensor networks, Electronics Letters, Vol. 50, Issue 12, PP. 894-896, (2014)

[3] Asma Mesmoudi, Mohammed Feham, Nabila Labraoui, Wireless Sensor Networks Localization Algorithms: A Comprehensive Survey, International Journal of Computer Networks & Communications (IJCNC) Vol.5, Issue 6, PP. 45-64, (2013)

[4] H. Dai, A. G. Chen, X. F. Gu and L. He, Localization algorithm for large-scale and low-density Wireless sensor networks, Electronics Letters, Vol. 47, Issue 15, PP. 881-883, (2011)

[5] S. Goyal, T. Bhatia and A. K. Verma, Wormhole and Sybil attack in WSN: A review, 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, PP. 1463-1468, INDIACom (2015)

[6] X. Lin, "CAT: Building Couples to Early Detect Node Compromise Attack in Wireless Sensor Networks," GLOBECOM 2009 - 2009 IEEE Global Telecommunications Conference, Honolulu, HI, PP. 1-6, IEEE (2009)

[7] Wenbo Yang, Wen Tao Zhu, Voting-on-Grid Clustering for Secure Localization in Wireless Sensor Networks, IEEE Icc 2010 proceedings, PP-01-05, IEEE (2010)

[8] X. Huang, M. Ahmed and D. Sharma, Protecting from Inside Attacks in Wireless Sensor Networks, IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing, Sydney, NSW, PP. 186- 191, IEEE (2011)

[9] G. Han, J. Jiang, C. Zhang, T. Q. Duong, M. Guizani and G. K. Karagiannidis, A Survey on Mobile Anchor Node Assisted Localization in Wireless Sensor Networks, IEEE Communications Surveys & Tutorials, Vol. 18, Issue 3, PP. 2220-2243, IEEE (2016)

[10]Haafizah Rameeza Shaukat, Fazirulhisyam Hashim, Aduwati Sali, and M. Fadlee Abdul Rasid, Node Replication Attacks in Mobile Wireless Sensor Network: A Survey, International Journal of Distributed Sensor Networks Vol. 2014, Article ID 402541, PP-01-15, (2014)

[11]Ismail G¨uvenc, Chia-Chin Chong, A Survey on TOA Based Wireless Localization and NLOS Mitigation Techniques, IEEE Communications Surveys & Tutorials, Vol. 11, Issue 3, PP 107-124, IEEE (2009)

[12]K. Yu ,Y.J. Guo, Anchor-free localization algorithm and performance analysis in wireless sensor Networks, IET Commun., 2009, Vol. 3, Issue 4, PP. 549–560, IEEE (2009)

[13]Zhi-Ting Lin, Yu-Gui Qu, Li Jing, and Bao-Hua Zhao: AP Web Workshops 2006 Compromised Nodes in Wireless Sensor Network, Springer PP-224-230, Springer (2006)

[14]Mohamed-Lamine Messai, Classification of Attacks in Wireless Sensor Networks, International Congress on Telecommunication and Application'14 University of A.MIRA Bejaia, Algeria, PP 23-24, (2014)

[15]V Bharath Srinivas et al, Spoofing Attacks in wireless Sensor Networks, IJCSET, Vol. 3, Issue 6, PP. 201-210, (2013)

[16]Azzedine Boukerche, Horacio A. B. F. Oliveira, Eduardo F. Nakamura, Antonio A. F. Loureiro, Secure Localization Algorithms for Wireless Sensor Networks, IEEE Communications Magazine, Vol-08, PP – 96- 101, IEEE (2008)

[17]T. Meena, M. Nishanthy and E. Kamalanaban, Cluster-based mechanism for multiple spoofing Attackers in WSN, International Conference on Information Communication and Embedded Systems (ICICES2014), Chennai, PP. 1-5, (2014)

[18]S. H. Hong, B. K. Kim and D. S. Eom, Localization algorithm in wireless Sensor networks with network mobility, IEEE Transactions on Consumer Electronics, Vol. 55, Issue 4, PP. 1921-1928, (2009)

[19]Hui Song et al, Sensor node compromise detection: the location perspective, WCMC'07, PP-242- 247, (2007)

[20]Yuan Zhang,Wenwu Wu, and Yuehui Chen, A Range Based Localization Algorithm for Wireless Sensor Networks, Journal Of Communications And Networks, Vol. 7, Issue 4, PP – 429, (2005)

[21]Https://www.codeproject.com/articles/606364/wireless-sensor-network Localization-simulator-v