ISSN No. 0976-5697

Volume 7, No. 6(Special Issue), November 2016

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Efficient Mechanisms for Secure Wireless Sensor Network- A Survey

Ankita Singla
CS Department
Guru Nanak College
Budhlada, India

Deepali
CS Department
Guru Nanak College
Budhlada, India

Abstract— *In different application areas Wireless sensor network (WSN) is used. But during data transmission in WSNs there are some intruders present who may attack data for their benefits. Therefore this may affect on the performance of WSN. In this paper, we discussed and compared the different mechanisms providing security in WSN.*

Keywords— *LEACH, RPK, IDS, DRP, NRRP, MTRP*

I. INTRODUCTION

WSN has sensor nodes which sense different environmental parameters such as temperature, pressure, pollution etc. and send the collected data to sink [1]. But while transmitting data before it reached at sink intruders may attack the data for their own benefits. Therefore this leads an inefficient WSN. To provide security in WSN, data encryption is an efficient technique as shown in fig 1.

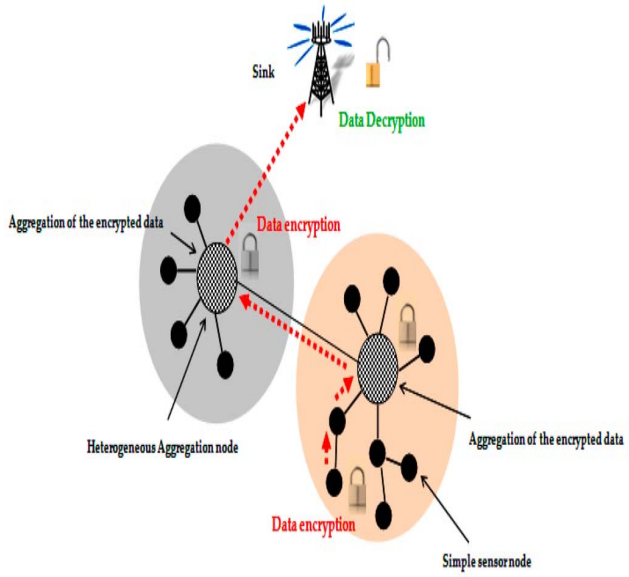

Fig 1 Security in WSN using Encryption Technique

An outline of this paper is as follows. Section II presents the RELATED WORK. Section III presents comparison of protocols and section IV describes the conclusion of the paper.

II. RELATED WORK

2.1 A secure routing protocol for cluster based Wireless Sensor Networks using Group Key Management

In [2] authors proposed RLEACH protocol to provide security in LEACH [3] protocol by improving RPK (Random pair-wise Key) [4] scheme. In this protocol sensor nodes select keys randomly and share with their neighbors for secure connection. After sharing keys, cluster heads (CHs) are elected in similar way as in LEACH. But sensor nodes select their CH based on condition that CH has shared key. If there are many CHs who have shared key then sensor nodes select that CH which has more signal strength. Hence this protocol provides secure connection with-in cluster. Then CHs will send data to sink using TDMA schedule. After receiving data sink ensures if data is valid by seeing original key and ID of CHs.

2.2 On the Intruder Detection for sinkhole attack in Wireless Sensor Networks

In [5] authors proposed an algorithm to locate intruders in WSN. In WSN, sink finds an affected area by calculating inconsistency in data. But all sensor nodes are not intruder in affected area therefore real intruder and some malicious nodes which help intruder by providing wrong information to sink are located by observing routing information or by using encryption and path redundancy methods.

2.3 Decentralized Intrusion Detection in Wireless Sensor Networks

In [6] authors proposed intrusion detection system (IDS) in WSN. In this system some sensor nodes are called monitor node in which IDS functionality is added to locate intruder. IDS in monitor nodes have three phases. First phase is *data acquisition* in which important data collected from neighbor nodes by monitor node is filtered out. Second phase is *Rule Application* in which some rules are applied on data to calculate data failure if data is not satisfied on applied rules. Third phase is *Intrusion Detection* in which number of data failures in present is compared with previous record. If current data failures are high than previous it means intrusion is present. Hence monitor nodes will discard that data.

2.4 Secure data collection in Wireless Sensor Networks using Randomized Dispersive Routes

In [7] authors proposed multi-path routing mechanisms in WSN to provide security by selecting data transmission path randomly for each packet of data. In randomized multi-path routing mechanism source sensor node sets TTL which is a counter value stores maximum number of sensor nodes that would carry packet of data to sink in multi-hop manner. Firstly source node selects its neighbor node randomly to send packet

978-93-85670-72-5 © 2016 (RTCSIT)

CONFERENCE PAPER
International Conference on
Recent Trends in Computer Science & Information Technology (RTCSIT-2016)
21st August 2016
Guru Nanak College Budhlada, Punjab India

of data and after transmitting packet will decrement the value of TTL by 1. Then neighbor node do same as source node by selecting its neighbor node randomly and process continues until values of TTL becomes 0. But there is a problem of redundancy, as neighbor nodes are selected randomly therefore there are many chances of selection of previous selected sensor nodes therefore authors have proposed various mechanisms DRP (Directed Random Propagation), NRRP (Non-repetitive Random Propagation), MTRP (Multicast Tree-assisted Random Propagation) to avoid redundancy problem.

2.5 On the security of cluster-based communication protocols for Wireless Sensor Networks

In [8] authors proposed SLEACH protocol to provide security in WSN by improving LEACH [3]. CHs are elected in similar way as in LEACH. But there may be some intruders can be elected as CHs. Therefore to avoid this CHs will have symmetric key to be shared with sink for authentication purposes. Sink will broadcast message to sensor nodes about authenticated CHs. Then sensor nodes will select their CH according to signal strength and further cluster head will send data to sink.

2.6 LEAP: Efficient Security Mechanisms for Large Scale Distributed Sensor Networks

In [9] authors proposed localized encryption and authentication protocol (LEAP) to add security in WSN by introducing four type of keys- *individual key* which is shared by sensor nodes with sink, *pair wise key* which is shared between two sensor nodes, *cluster key* which is shared with all neighbor nodes of sensor node and *group key* which is shared by all sensor nodes in WSN. This protocol provides different type of keys to reduce key management process and add authentication by using one way key-chain.

2.7 SRDA: Secure Reference-Based Data Aggregation Protocol for Wireless Sensor Networks

In [10] authors proposed SRDA protocol to provide security in cluster based WSN. In this protocol distance between sink and CHs is calculated using deployment information and encryption is applied on data. Authors have also introduced reference based data aggregation technique to reduce data transmission overhead from sensor nodes to CHs by sending only reference data instead of full details. Hence this protocol provides security as well as less communication cost.

2.8 Energy Efficient Security Protocol for Wireless Sensor Networks

In [11] authors introduce Non-blocking Orthogonal Variable Spreading Factor (NOVSF) [12] code hopping technique to provide security in cluster based WSN. In this protocol security is enhanced with key distribution scheme and NOVSF technique where different time slots are allotted to sensor nodes for data transmission to CHs at each round. Sensor nodes first encrypt the data and then set time slot by applying NOVSF code hopping technique. Hence intruder would need more time to find out pattern at each round.

2.9 SEDAN: Secure and efficient data aggregation protocol for Wireless Sensor networks

In [13] authors proposed an efficient protocol SEDAN to provide security as well as enhance energy efficiency in WSN by introducing two-hop pair wise key. In WSN data is transmitted in multi-hop manner by sensor nodes to sink using data aggregation technique. Parent sensor node collects aggregated data from its neighbor child sensor nodes and further sends data to its neighbor sensor node which is grandparent of its child nodes. Hence two-hop pair wise key is shared between only child and grandparent sensor nodes but parent node is not aware of this shared key. With the help of this key verification of sensor nodes is done by sensor nodes itself, thus reduce the load of sink node for verification process which makes protocol energy efficient as packets sent by sink node for verification of sensor nodes are not needed.

2.10 A new scheme of key distribution using implicit security in Wireless sensor networks

In [14] authors proposed a new scheme where sink node distributes the key partitions randomly to each sensor node in WSN. When any user requests for data then sensor nodes which are interested to process request are acknowledged to sink node. After getting acknowledgement sink node computes path key and distributes the path key to interested sensor nodes. Then sensor nodes encrypt data using path key and transmit it to sink node.

2.11 Location-aware key management scheme for wireless sensor networks

In [15] authors proposed structured key-pool random key pre-distribution (SK-RKP) scheme where two type of keys are distributed among sensor nodes. First kind of key is shared by sensor node with its neighbor nodes that belong to same area. Second kind of key is shared by sensor node with its neighbor nodes that belong to different area.

2.12 Efficient tracing of failed nodes in sensor networks

In [16] authors proposed secured protocol to find out malicious sensor node. In this protocol, sensor nodes send the information about their neighbor nodes to sink node. This acknowledges the sink node about the topology of network. Therefore sink node can detect malicious node by applying divide and conquer method to update routing information to sensor nodes.

2.13 Feedback: Towards dynamic behavior and secure routing for wireless sensor networks

In [17] authors proposed feedback based secure routing (FBSR) protocol to provide security in WSN by having feedback about sensor nodes from their neighbor nodes and sink node. In this protocol, a sensor node send data to sink node after deciding

978-93-85670-72-5 © 2016 (RTCSIT)
CONFERENCE PAPER
International Conference on
Recent Trends in Computer Science & Information Technology (RTCSIT-2016)
21st August 2016
Guru Nanak College Budhlada, Punjab India

routing path on the basis of feedback containing reliability, residual energy, reputation of other sensor nodes collected from its neighbor nodes.

2.14 An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks

In [18] authors proposed a witness-based scheme where aggregated data is sent to sink node by sensor nodes. In this scheme some sensor nodes are selected as witnesses to monitor sensor node which have aggregated data and that data is sent to sink node along with its witness information. When data is received by sink node it decides whether witness information about sensor node is correct or not by using voting system.

III. PROTOCOL COMPARISON

The papers surveyed have worked on different security mechanisms in WSN. Protocols discussed in above section are compared and presented in Table 1.

Protocols	***Data Transmission***	***Energy Efficiency***	***Cluster-based Protocol***
[2]	Single-hop	Good	Yes
[5]	Multi-hop	Good	No
[6]	Multi-hop	Good	No
[7]	Multi-hop	Very Good	No
[8]	Single-hop	Very Good	Yes
[10]	Single-hop	Very Good	Yes
[11]	Single-hop	Very Good	Yes
[12]	Multi-hop	Very Good	No
[13]	Multi-hop	Good	No
[14]	Multi-hop	Good	No

TABLE I. COMPARISON OF SECURITY MECHANISMS IN WSN

IV. CONCLUSION

WSN in different application areas is widely used for continuous monitoring of environment parameters. But in WSN while transmitting data from sensor nodes to sink intruders may attack the data for their own benefits. Therefore this leads an inefficient WSN. In this paper, we presented the various protocols proposed security mechanisms in WSN and we compared these protocols.

REFERENCES

[1] I.F.Akyildiz,W. Su, Y. Sankarassubramaniam, E.Cayirci, “Wireless Sensor Networks: a survey,” Computer Networks(Elsevier), vol. 38, pp. 393-422, 2002.

[2] K. Zhang, C. Wang and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," *2008 4th International Conference on Wireless Communications, Networking and Mobile Computing*, Dalian, 2008, pp. 1-5. doi: 10.1109/WiCom.2008.889

[3] W.R.Heinzelman,“Energy-Efficient Communication Protocol for Wireless Microsensor Networks,” Proc. of the 33rd Hawaii International Conference on System Sciences, pp. 1-10, 2000.

[4] Chan H, Perrig A, Song D. Random key pre-distribution schemes for sensor networks. In Proceedings of the IEEE Computer Society Symposium on Security and Privacy. Piscataway, USA: IEEE, pages 197-213, 2003.

[5] E. C. H. Ngai, J. Liu and M. R. Lyu, "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks," *2006 IEEE International Conference on Communications*, Istanbul, 2006, pp. 3383-3389. doi: 10.1109/ICC.2006.255595

[6] Ana Paula R. da Silva, Marcelo H. T. Martins, Bruno P. S. Rocha, Antonio A. F. Loureiro, Linnyer B. Ruiz, and Hao Chi Wong. 2005. Decentralized intrusion detection in wireless sensor networks. In *Proceedings of the 1st ACM*

international workshop on Quality of service & security in wireless and mobile networks (Q2SWinet '05). ACM, New York, NY, USA, 16-23. DOI=http://dx.doi.org/10.1145/1089761.1089765

[7] T. Shu, M. Krunz and S. Liu, "Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes," in *IEEE Transactions on Mobile Computing*, vol. 9, no. 7, pp. 941-954, July 2010. doi: 10.1109/TMC.2010.36

[8]Adrian Carlos Ferreira, Marcos Aurélio Vilaça, Leonardo B. Oliveira, Eduardo Habib, Hao Chi Wong,Antonio A. Loureiro “On the Security of Cluster-Based Communication Protocols for Wireless Sensor Networks” Networking - ICN 2005: 4th International Conference on Networking, Reunion Island, France, April 17-21, 2005, Proceedings, Part I 2005 Springer Berlin Heidelberg 978-3-540-31956-6 Ferreira2005 10.1007/978-3-540-31956-6_53 http://dx.doi.org/10.1007/978-3-540-31956-6_53 449-458

[9] Sencun Zhu, Sanjeev Setia, and Sushil Jajodia. 2006. LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. *ACM Trans. Sen. Netw.* 2, 4 (November 2006), 500-528. DOI=http://dx.doi.org/10.1145/1218556.1218559

[10] H. O. Sanli, S. Ozdemir and H. Cam, "SRDA: secure reference-based data aggregation protocol for wireless sensor networks," *Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th*, 2004, pp. 4650-4654 Vol. 7.doi: 10.1109/VETECF.2004.1404972

978-93-85670-72-5 © 2016 (RTCSIT)

CONFERENCE PAPER
International Conference on
Recent Trends in Computer Science & Information Technology (RTCSIT-2016)
21st August 2016
Guru Nanak College Budhlada, Punjab India

[11] H. Cam, S. Ozdemir, D. Muthuavinashiappan and P. Nair, "Energy efficient security protocol for wireless sensor networks," *Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th*, 2003, pp. 2981-2984 Vol.5.doi: 10.1109/VETECF.2003.1286170

[12] H. Cam, "Nonblocking OVSF Codes and Enhancing Network Capacity for 3G Wireless and Beyond Systems", To appear in the Special Issue of Computer Communications on "3G Wireless and Beyond For Computer Communications", Spring 2003.

[13] X. Wang, J. Li, X. Peng and B. Zou, "Secure and Efficient Data Aggregation for Wireless Sensor Networks," *Vehicular Technology Conference Fall (VTC 2010-Fall), 2010 IEEE 72nd*, Ottawa, ON, 2010, pp. 1-5.doi: 10.1109/VETECF.2010.5594524

[14] Chien-Wen Chiang, Chih-Chung Lin and Ray-I Chang, "A new scheme of key distribution using implicit security in Wireless Sensor Networks," *Advanced Communication Technology (ICACT), 2010 The 12th International Conference on*, Phoenix Park, 2010, pp. 151-155.

[15] D. Huang, M. Mehta, D. Medhi, and L. Harn, "Location-aware key management scheme for wireless sensor networks," in *Proc. 2nd ACM Sorkshop on Security of Ad hoc and Sensor Networks*, 2004, pp. 29–42

[16] J. Staddon, D. Balfanz, and G. Durfee, "Efficient tracing of failed nodes in sensor networks," in *Proc. 1st ACM International Workshop Wireless Sensor Networks Applications*, 2002, pp. 122–130

[17] Z. Cao, J. Hu, Z. Chen, M. Xu, and X. Zhou, "Feedback: Towards dynamic behavior and secure routing for wireless sensor networks,"in *Proc. 20th International Conf. Advanced Information Networking Applications (AINA)*, 2006, vol. 2, pp. 160–164.

[18] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-byhop authentication scheme for filtering of injected false data in sensor networks," in *Proc. IEEE Symposium Security Privacy*, 2004, pp. 259–271.

978-93-85670-72-5 © 2016 (RTCSIT)

CONFERENCE PAPER
International Conference on
Recent Trends in Computer Science & Information Technology (RTCSIT-2016)
21st August 2016
Guru Nanak College Budhlada, Punjab India