INFOGAIN PUBLICATION

International Journal of Advanced Engineering, Management and Science (IJAEMS)
Peer-Reviewed Journal
ISSN: 2454-1311 | Vol-7, Issue-11; Nov, 2021
Journal Home Page: https://ijaems.com/
Article DOI: https://dx.doi.org/10.22161/ijaems.711.1

Efficient Data Aggregation in Wireless Sensor Networks

Susan Mary Olakkengil[1], Dr. Subhas Singh Parihar[2]

[1]Scholar, Dept of Computer Science Engineering, North East Frontier Technical University, Arunachal Pradesh, India
[2]Professor, Dept of Computer Science, North East Frontier Technical University, , Arunachal Pradesh, India

Received: 03 Oct 2021; Received in revised form: 01 Nov 2021; Accepted: 08 Nov 2021; Available online: 16 Nov 2021

Abstract— *Sensor network is a term used to refer to a heterogeneous system combining tiny sensors and actuators with general/special-purpose processors. Sensor networks are assumed to grow in size to include hundreds or thousands of low-power, low-cost, static or mobile nodes. This system is created by observing that for any densely deployed sensor network, high redundancy exists in the gathered information from the sensor nodes that are close to each other we have exploited the redundancy and designed schemes to secure different kinds of aggregation processing against both inside and outside attacks.*
***Keywords*— Sensor network, data aggregation, wireless sensor.**

I. INTRODUCTION

"Sensor network" is a term used to refer to a heterogeneous system combining tiny sensors and actuators with general/special-purpose processors. Sensor networks are assumed to grow in size to include hundreds or thousands of low-power, low-cost, static or mobile nodes.

Sensor networks are useful in a variety of fields, including environmental monitoring, military surveillance, and information gathering from inhospitable places. They not only monitor but also facilitate control of physical environments from remote locations. Sensors play important roles in various applications: measuring flow, temperature, humidity, pressure, brightness, mechanical stress, and proximity. Areas such as disaster anticipation, environment control, health care, military command control benefit greatly from this emerging technology.

High priorities, leading to the question of to what degree the network is secure? So far, most of the research has focused on making sensor networks a reality. Security, relatively speaking, has not received as much concern primarily because of the difficulty of dealing with such devices under stringent specifications. Traditionally, security relies heavily on cryptographic methods; nevertheless, a significant number of problems require security specification that is beyond the scope and ability of all known cryptographic techniques.

In this paper, we proposed a Framework for secure Data Aggregation approach. This approach is able to detect malicious sensors, assign trust values to each sensor, and apply cryptographic techniques to achieve Security Principles

This paper is organized as follows: Section 2: explains literature survey, different methodologies on wireless sensor networks, their nature, applications, and typical paradigms; Section 3: contains the two main concepts, security in sensor networks, and data aggregation techniques in sensor networks. Section 4: depicts the details of the proposed approach to achieving secure data aggregation. Section 5: Results. 6: Finally, conclusions are drawn in.

II. RELATED WORK

Wagner et. aL, in [2], show a number of examples in which simple attacks were able to bring down a network running some known routing protocols, for example, TinyOS beaconing protocol. This protocol constructs a breadth first spanning tree rooted at a base station. A route update is initiated at the root and broadcast to the neighboring nodes, which, in turn, propagate the same update to the other nodes. Each node marks the sender as a parent node (Figure 2.1).

©2021 The Author(s). Published by Infogain Publication.
This work is licensed under a Creative Commons Attribution 4.0 License. http://creativecommons.org/licenses/by/4.0/

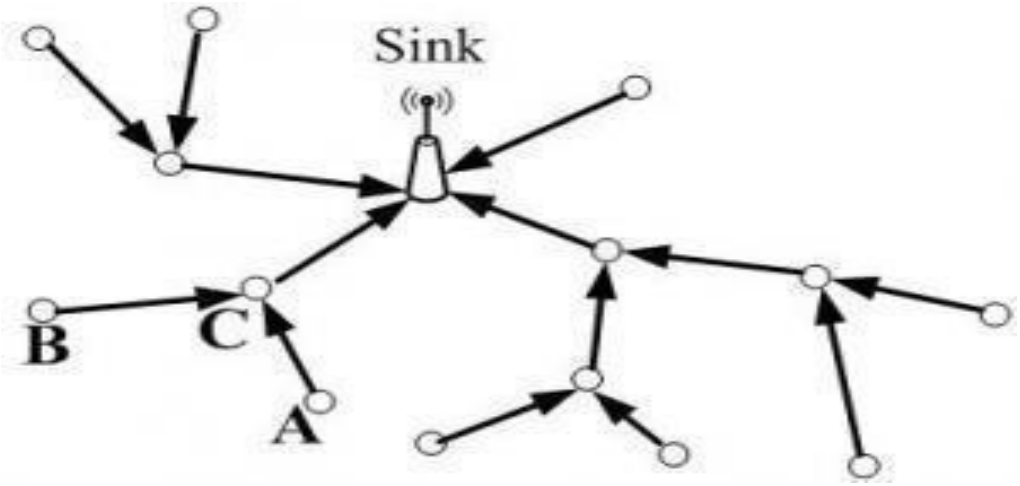


Fig.2.1 A WSN Constructed Using TinyOS

2.1 Sensor Networks

Sensor networks rely on sensing, processing and wireless communication abilities. Thanks to recent enhancements and developments in electronics, sensor networks have greater flexibility in terms of the solutions they can offer in a wide range of applications. Their extent application is only limited by the availability of the sensing elements that can be employed. Some of the sensors used today include those that measure temperature, pressure, humidity, flow, vibration, brightness, mechanical stress, and proximity. Thus, sensor networks are well suited to a variety of monitoring and surveillance applications

The development of sensor nodes (hardware and software) has been greatly influenced by the type of application they serve. Generally, sensor nodes must be small, economical, energy efficient, equipped with sensing elements, good at computation performance, and have suitable wireless communication facilities. Figure 2.2 shows the main hardware components that build a typical sensor node: processor, memory, sensors, communication elements, and power supply [5,6,7]. However, it is important to note that some applications may require extra hardware components, for example, a GPS to locate a node, or UAVs to move a node, or a power generator.

2.2 Sensor Hardware Considerations

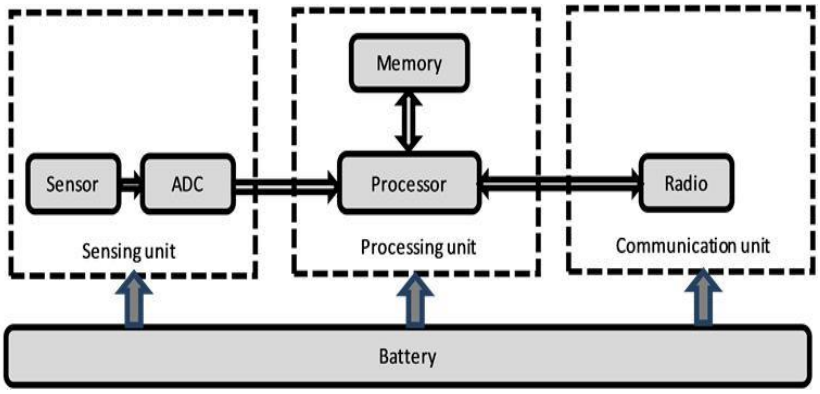
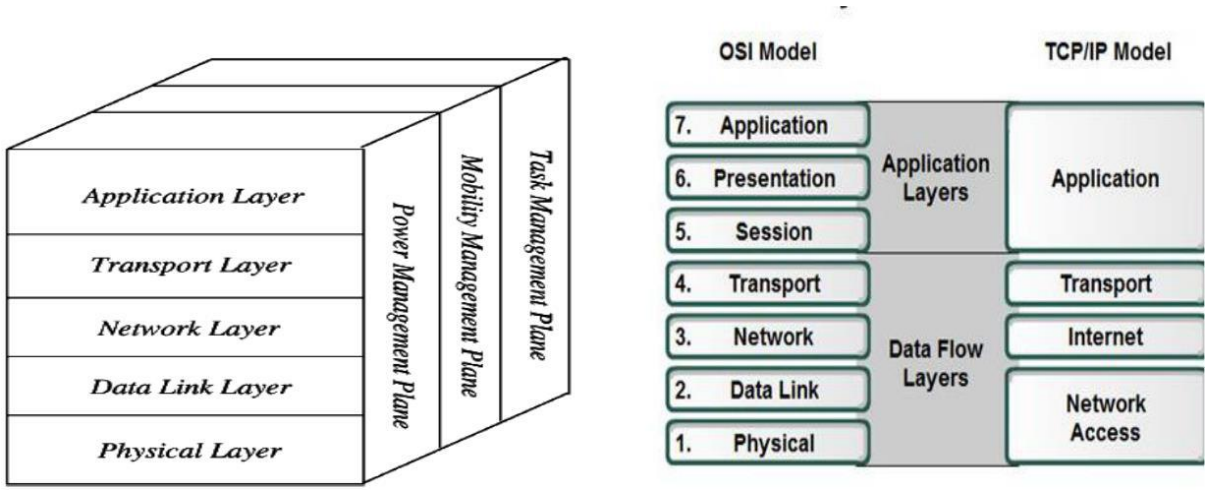


Fig.2.2: Sensor Node Hardware Components

2.3 Sensor Node Communication Architecture (Protocol Stack)

Similar to all other communication devices, sensor network design complies with the layer design approach, in which every layer has to provide well-defined functionalities. According to [8], the protocol stack consists of the physical layer, data link layer, network layer, transport 1and application layer (Figure 2.3),

©2021 The Author(s). Published by Infogain Publication.
This work is licensed under a Creative Commons Attribution 4.0 License. http://creativecommons.org/licenses/by/4.0/



(a) Protocol Stack (b) Cross-layer

Information exchange

Fig.2.3: Sensor Network Communication Architecture

2.4 Challenges: Sensor Capability and Security

Poor Resources (memory, processor, and power): as can be inferred from Table 1 above, sensors are deprived of the luxury of having strong resources, similar to all other networks, to run security algorithms, which demand a certain amount of resources memory space for the code and data, processing power, and energy. Therefore, security algorithms code has to be kept small, which may involve modification and optimization to ' traditional security functions

Unreliable Communication: communication between sensors is not reliable, mainly suffering from collisions, latency, and the connectionless nature of packets routing.

Error rate in wireless sensor networks by default is high, leading to packet loss and damage. Software developers are required to handle errors by incorporating the mechanism for that, such as error detection and correction.

Unattended Operation: in most cases, once sensors are deployed, they are left unattended, behind enemy lines in some cases, management, for example, may take place remotely. As a result, physically tampering with sensors is very likely to happen and detection is extremely difficult.

III. SECURITY AND DATA AGGREGATION INWSNS

With the importance of in-network processing, however, enforcing security becomes a more challenging task. As a matter of fact, data aggregation techniques and security protocols face conflicts in their implementation. On one side, to eliminate redundancy of data and thereby reduce the number of packets transmitted in the network, the data aggregation protocols require sensor data to be processed by the intermediate nodes as much as possible. Therefore, data should be available in the clear text at every intermediate node to perform the aggregation process. On the other side, security protocols commonly require that sensor nodes encrypt any data prior to transmission so that information confidentiality is achieved. Data aggregation cannot

be sacrificed. Its high importance in reducing redundancy, expanding network lifetime, and enhancing data accuracy necessitates its implementation. However, both data aggregation

and false data infection cause sensor data modification, so legitimate data and false data can be confused. For those reasons, false data detection, compromised node elimination, and data aggregation protocols should be designed together so that the sensor network can survive and work successfully.

3.1 Homomorphic Encryption

The Homomorphic encryption as originally introduced by Claude et al [16], Homomorphic encryption schemes are especially useful in scenarios where someone who does not have decryption keys needs to perform arithmetic operations on a set of ciphertexts.

3.2 Cryptographic Hash Function

A cryptographic hash function is a deterministic procedure that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that an accidental or intentional change to the data will change the hash value. The data to be encoded is often called the

©2021 The Author(s). Published by Infogain Publication.
This work is licensed under a Creative Commons Attribution 4.0 License. http://creativecommons.org/licenses/by/4.0/

"message", and the hash value is sometimes called the message digest or simply digests.

IV. PROPOSED APPROACH TO ACHIEVE SECURE DATA AGGREGATION

This approach is able to detect malicious sensors, assign trust values to each sensor, and apply cryptographic techniques to achieve Security Principles. The chapter is organized as follows:

1) System Model and Assumptions: This section explains some basic assumptions about the sensor network setup. Furthermore, it states the thesis goal from a security point of view.

2) Solution Framework: This part presents a strategy to achieve confidentiality, Integrity and authentication in data aggregation in WSN.

3) Performance Analysis: This section evaluates the performance of the proposed secure aggregation method. Performance evaluation involves simulation results, and energy savings.

4.1 SYSTEM MODEL AND ASSUMPTIONS

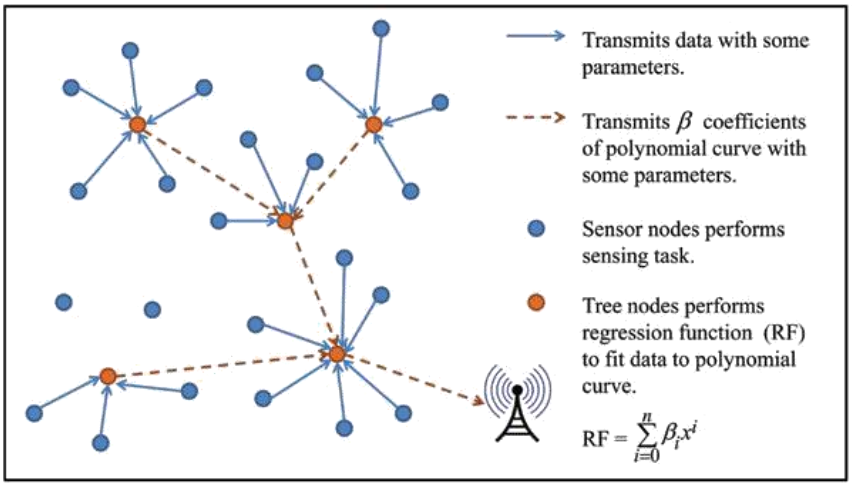


Fig.4.1 Aggregation Network

4.2 Security Goal and Assumptions

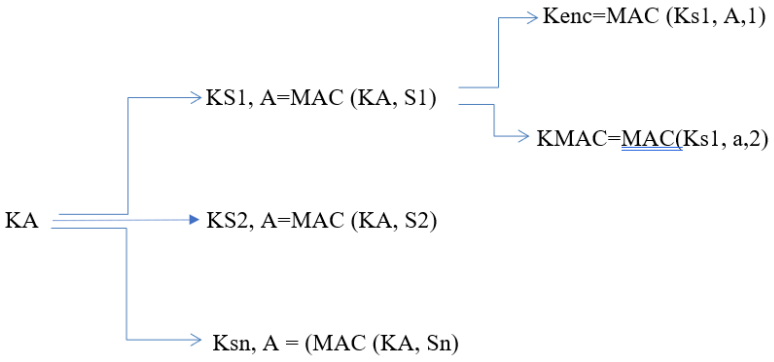
Consider the scenario of a network of wireless sensors deployed in a certain area to perform measurements. Because the sensors are assumed to be simple, low in power consumption, and short in communication range, there exist intermediate nodes with relatively higher processing capabilities called aggregators. Upon a query from the home server, sensors perform their measurements and report to the aggregator, Which, in turn, performs some processing and eventually sends the result to the home server (Figure 4-1).

THE SECURE DATA AGGREGATION PROTOCOL

4.2.1 Key Setup

Initially, cryptographic tools and secret keys are installed on all sensors; however, the use of them is avoided until misbehavior is detected.

- n is the number of nodes.
- S1,……Sn are the regular nodes.



©2021 The Author(s). Published by Infogain Publication.
This work is licensed under a Creative Commons Attribution 4.0 License. http://creativecommons.org/licenses/by/4.0/

The following are the notations :

- H is the home server or base station.
- A is the aggregator.
- Xi is the value reported by Si.
- KH,Si is the shared key between sensor i and the home server.
- KA,Si is the shared key between the aggregator and home server.
- E(K,m) refers to the encryption of message m using key K.
- MAC(K,m) is the message authentication code of message m with key K.
- Si:m means a sensor Si sends a message m to the aggregator A. In a similar manner, A .n and H .n are defined.
- Agg is the aggregate result that the aggregator node produces.

4.2.2 Deriving keys from the master secret key

If a new node is added to the system, the corresponding key is added in the system, to the home server, and to the aggregator. However, for security reasons, the aggregator key can be changed and disseminated to all the nodes When needed. Nodes communicate. with the home server through the aggregator. In parts of our communication protocol, the nodes exchange special information with the home server using the home server node keys. Even though communication takes place through the aggregator, obviously the latter is not able to reveal such information. Communication between neighbouring nodes is not part of the current set-up, so pair-wise key sharing is not required.

4.2.3 Communication Messages

START is the message used by home server. Initially, Horne server broadcasts this message to all the sensor nodes in the field to indicate that all nodes should start their task.

HELLO is the message broadcasted by all the nodes after receiving START message, in order to find their neighbours. This message will reach to those nodes only that are within range of that node.

REPLY is the message send by a node when it' receives HELLO message. This message contains the node id. After receiving the REPLY message, each node makes it neighbour list. Initially a node has empty neighbour list. When a node replies with its ID, then node receiving REPLY message retrieves the ID and make entry in its neighbour list.

STATUS is the message send to Home Server either directly or via aggregator. It contains neighbour list, residual energy of the node. After collecting the neighbour information, each node sends STATUS message to the home server.

ACK is the acknowledgement send by the home server name server and those nodes which receives STATUS message. That means when home server receives STATUS message directly it sends back an ACK message. Or when a node (Aggregator) have STATUS message, It also sends back an ACK message to acknowledge them that STATUS has been successfully received.

AGG_ADV is the message used to advertise the nodes themselves as a Aggregator. Actually, if the home server in the range of nodes then those nodes can send their STATUS to home server directly. But in the case if it is not within their range, then nodes need to have their aggregators to send their STATUS up to home server.

When a node receives ACK message, then it advertises itself as an Aggregator by sending AGG_ADV message. A node receiving AGG_ADV, sends their STATUS to aggregator advertising node. In this case, a node can receive AGG_ADV message from many nodes. But it sends their STATUS to only that node from where it has received AGG_ADV message early.

4.3 Secure Hierarchical Aggregation

If the sensor network is too large, which is common, then multiple aggregators, usually cooperating, are required to handle the entire network. Functions such as AVERAGE, MIN, and MAX do support hierarchical aggregation. That 'is, every aggregator performs the aggregation function on a subset of the nodes in the sensor network. The results are collectively sent to other aggregators for computing the same aggregation function again,

The proposed algorithm has mainly three broad phases

a) Setup phase

b) Security Phase

c) Transmission Phase

4.3.1 Setup Phase

In this phase, cluster set up, aggregator selection and Aggregator to Aggregator routing path is to be set up which is done using the communication messages.

4.3.2 Security Phase

Step 1: When an interesting event occurs, sensor node encrypts the result with homomorphic encryption as shown below

E (K, m) =Xi + KH, Si mod M

©2021 The Author(s). Published by Infogain Publication.
This work is licensed under a Creative Commons Attribution 4.0 License. http://creativecommons.org/licenses/by/4.0/

Where Xi is reading of sensor node, KH, Si is shared key between home server and sensor node and M = number of nodes * maximum possible value of reading.

Step 2.: Sensor node calculates the MAC of the given message using shared key between sensor and aggregator.

4.3.3 Transmission phase

Every Aggregator node informs each one of its child nodes when it can transmit, according to the TDMA schedule which is broadcasted back to the nodes in the cluster. Each node, during its allocated transmission time, sends to the cluster head quantitative data concerning the sensed events. Sensors to Aggregator Data Transmission Data aggregation flows starts from the regular nodes and ends at the home server. Again, in a trusted environment, sensors send simple packets that carry their IDs and readings to the aggregator.

The secret key used here is the one shared between the node and the aggregator. The following shows the packet that a regular node Si, sends to the aggregator.

Si, E (KSi, H, Xi | NH) | MAC (KSi, A, si | Xi| NH), where Xi is the data reported by node Si, and NH is a random number to identify the query and to prevent replay attacks.

The home server collects all the messages transmitted to it. The home server determines the new cluster heads by using the data of the received message. More precisely, the node having the highest residual energy and maximum number of neighbors, in each cluster, is elected to be the new aggregator.

V. RESULTS

5.1 Energy Consumption

One contribution in favor of our security scheme is the conservation of energy it makes. Cryptography causes considerable extra consumption energy, mainly due to packet overhead, which leads consequently to a shorter network lifetime. The exact amount of energy saved depends on the security requirements, encryption and/ or authentication, and the implemented cryptographic primitives, such as RC5, RC6, and DES.

Table 1 demonstrates the costs of computation and communication in terms of energy. Most of the overhead is related to the transmission of the extra bytes rather than computations.

Table 1: Energy Costs of Adding Security Protocols

Packet Component		Energy Consumption (%)
Data Transmission		71
Encryption Computation		< 1
Encryption Transmission		< 1
MAC Computation		2
MAC Transmission		20

Table: 2 Radio Energy Costs

Security Option		Energy (mJ)	Increase (%)
No security		1.215	-
Authentication		1 .247	2 .6
Authentication	and	1.385	13.99
encryption			

Table 2 lists the security options and the corresponding energy consumption that is related to packet transmission.

In conclusion, Power efficiency is an important aspect, which directly influences network lifetime. By making the security choice and looking at the tables above, the security designer can estimate the amount of energy to spend.

5.2 Average Energy Dissipation

Figure 5.1 shows the average energy dissipation of the protocol under study over the number of rounds of operation. This plot clearly shows that WITHAGG has a much more desirable energy expenditure curve than that of NOAGG and WITH AGGnSEC. On average, Protocol WITHAGG exhibits a reduction in energy consumption of 30 percent to protocol with NOAGG. This is because of data aggregation no of message transfer are reduced. When we employ security then there is slight increase in energy consumption because much energy is required in communication than processing in sensor node.

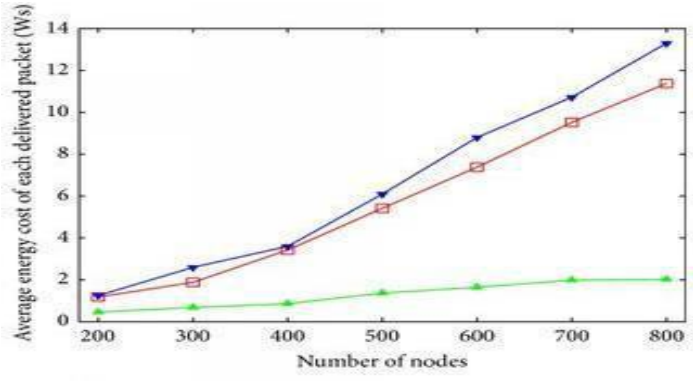


Fig.5.1: A Comparison of Avg Energy Dissipation of Protocol with Aggregation, No Aggregation and both Aggregation and Security

©2021 The Author(s). Published by Infogain Publication.
This work is licensed under a Creative Commons Attribution 4.0 License. http://creativecommons.org/licenses/by/4.0/

5.3 System life Time

The improvement gained through proposed protocol is further exemplified by the system lifetime graph in Figure 5.2. This plot shows the number of nodes that remain alive over the number of rounds of activity for the 100 m X 100 m network scenario. For Protocol with aggregation, 82% of the nodes remain alive for 60 rounds, while the corresponding numbers for protocol with No Aggregation is 40%, respectively. And With this, 45% of the nodes alive for 105 rounds while the corresponding numbers for protocol with no aggregation is 0 node alive i.e. all the nodes are dead for protocol with no aggregation after 105 rounds.

VI. CONCLUSION AND FUTURE WORK

6.1 Conclusion

Sensor networks promise viable solutions to many problems in a variety of fields. Sensing technology today is moving relatively fast from research contexts to industrial and social contexts, and with increased interest in implementing sensor networks, there comes a vital concern about data secrecy.

The motivation behind this research is to relax the conflict that applying security on sensor networks tends to compromise other important issues.

First, Cryptographic tools cause extra consumption of energy. Second, cryptographic functions assume that nodes are trustworthy as long as they use the assigned secret. keys. Third, end-to-end security prevents intermediate nodes from modifying message contents. Consequently, applying security does not allow data aggregation techniques to take place, deprives sensor networks of a long lifetime, and does not solve the inside attack problem. In spite of all that, security and data aggregation must both be implemented because they are vital for the success of sensor networks. In this context, this thesis addresses security issues in wireless sensor network, with a strong focus on secure data aggregation. A novel mechanism is proposed to achieve data aggregation while maintaining security requirements and preserving energy, even in the presence of Byzantine nodes (inside attacks).

In the proposed technique, the aggregator, in addition to performing the regular aggregation function, the sensor nodes maintains the integrity, authentication and confidentiality

However, it should be noted that the proposed mechanism has some limitations. Firstly, the maximum number of Byzantine nodes that this mechanism can simultaneously handle must be less than half of the total number of nodes. Secondly, it assumes that aggregator nodes are trustworthy. Thus, for this mechanism to work efficiently, the aggregators must be provided with a higher level of security, such as Tamper-resistant packaging, and be placed in secure locations. Thirdly, a master key is used in deriving other keys for. all sensors to use. This keying technique introduces a shortcoming: if the master key is compromised, then the whole network can be compromised.

6.2 Future Work

The future works is to add the aggregator node to the list of non-trustees. In this thesis, the aggregator is regarded as a trusted node, which satisfies many sensor network applications. However, it is also of interest to determine the aggregator's honesty. For that, another mechanism should be added. Chapter 3 introduces some work done in this area, detecting a malicious aggregator. For example, Deng et a1. [50] and Wu et a1. [51] propose having watchdog-like nodes to monitor the aggregators. These techniques can be manipulated so that they integrate with m}; technique. Moreover, an interactive proof technique in which the home server ensures that the aggregator is not malicious is possible. That is, the home server investigates previous readings and assigns trust values to the aggregator based on them.

A second possible approach for extension is to implement multi-tiered security architecture. The proposed scheme assumes that cryptography is either on or off with multitiered security design, different levels of security can be maintained. Every security level can be triggered in accordance with the trust assessment.

To summarize, security protocols and data aggregation techniques seem to introduce conflicts; however, integrating them both is essential for the success of a sensor network. The results of this thesis provide a good starting point for a deeper study of secure data aggregation protocols.

REFERENCES

[1] On world at https: www.onworld.com html wirelesssensorsr-rtshtm

[2] C. Karlof and D. Wagner. Secure Routing in Sensor Networks: Attacks and Countermeasures. In Proc. , of First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.

[3] H. Karl and A. Willig. Protocols and Architectures for Wireless Sensor Networks. Wiley, 2005. ISBN20470095105.

[4] F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci. Wireless Sensor Networks: a Survey. Computer Networks (Amsterdam, Netherlands: 1999)

©2021 The Author(s). Published by Infogain Publication.
This work is licensed under a Creative Commons Attribution 4.0 License. http://creativecommons.org/licenses/by/4.0/

[5] S. Tilak, N. Abu-Ghazaleh, and W. Heinzelman. A Taxonomy of Wireless Microsensor Network Models. ACM Mobile Computing and Communications Review 2002. ‘

[6] K. Akkaya and M. Younis. A survey on routing protocols for wireless sensor networks. Elsevier Ad Hoc Network, Vol. 3 / 3zpages 325-349, 2005

[7] J . N. Al-Karak and A. E. Kamal. Routing techniques in wireless sensor networks: a survey. IEEE [Wireless Communications. Dec. 2004.

[8] F, Akyildiz, Y. Sankarasubramaniam, W. Su, and E.Cayirci. Wireless Sensor Networks: a survey. Computer Networks: The International Journal of Computer and Telecommunications Networking, Volume 38 Issue 4, March 2002.

[9] E. Sohrabi, “Protocols for self-organization of a wireless sensor network,” pp. 16-27, October 2000.

[10] Woo and D. Culler, “A transmission control scheme for media access in sensor networks,” July 2000.

[11] W. Heinzelman, J. Kulik, and H. Balakrishnan, “Adaptive protocols for information dissemination in wireless sensor networks,” pp. 174-185, 1999.

[12] C. Intanagowiwat, R. Govindan, and D. Estrin, “Directed diffusion: A scalable and robust communication paradigm for sensor networks,” pp. 56-67, 2000.

[13] 13].C. Shen, C. Srisatjapornphat, and C. Jaikaeo, “Sensor information networking architecture and applications,” IEEE Pers. Communication, pp. 52-59, Aug. 2001.

[14] Perrig, R. Szewczyk, D. ’I‘ygar, V. Wen, and D. Culler, "SPINS: Security protocols for sensor networks", Wireless Networks Journal (WINE), September 2002.

[15] S. Avancha, J. Undercoffer, A. Joshi, J. Pinkston. Security for Wireless sensor networks. ISBN: 1-4020-7883-8. pages 253-275. 2004. ‘

[16] L. Lamport, R. Shostak, and M. Pease, “The Byzantine Generals Problem”, ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3, July 1982, pp 382-410.

[17] Radia Perlmen, Routing with Byzantine Robustness, Sun Microsystems, Sep2005 '

[18] B. Awerbuch, R. Curtmola, D. Holmer, C. NitaRotaru, and H Rubens, “Mitigating Byzantine Attacks in Ad Hoc Wireless Networks,” Department of Computer Science, Johns Hopkins University, Tech. Rep. Version 1, March 2004.

[19] M. Pease, R. Shostak, L. Lamport, “Reaching Agreement in the Presence of Faults”, JACM 27, 2, 228-234, 1980. _

[20] M. Fischer and N. Lynch, “A Lower Bound for the Time to Assure Interactive Consistency”. Information Processing Letters 14, 4, 183-186, 1982.

[21] M. Fischer, N. Lynch, and M. Paterson, “Impossibility of Distributed Consensus with One Faulty Process”, JACM, 32, 2, 374-382, 1985. ,

[22] G. Guimaraes, E. Souto, D. Sadok, and J. Kelner, Evaluation of Security Mechanisms in Wireless Sensor Networks, Proceedirigs of the 2005 System Communications.

[23] M. Yu, S. Kulkarni, and P. Lau, “A New Secure Routing Protocol To Defend Byzantine Attacks For Ad Hoc Networks”, IEEE Int. Conf. on Networks (ICON’OS), vol. 2, pp. 1126-1131, Nov. 16-18, Kuala Lumpur, Malaysia.

[24] B. Awefbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, “An oh-demand secure routing protocol resilient to byzantine failures,” in ACM Workshop on Wireless Security (WiSe) 2002, 2002.

[25] G. Gaubatz, J.-P. Kaps, and B. Sunar, "Public key cryptography in sensor networks revisited", 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS2004L2004.

[26] H. Cam, S. Ozdemir, D. Muthuavinashiappan, and Nair, "Energy-efficient security protocol for wireless sensor networks", in Proc. of IEEE VTC Fall 2003 Conference, October 4-9, Orlando, 2003.

[27] C. Karlof, N. Sastry, and D. Wagner, "TinySec: A link layer security architecture for wireless sensor networks", Proc. of the Second ACM Conference on Embedded Networked Sensor Systems, November 3-5, Baltimore, 2004.

[28] Menezes, P. van Oorschot, and S. Vanstone. Handbook of Applied Cryptography, volume 6 of Discrete Mathematics and Its Applications. CRC Press, Greenwich, Connecticut, 1996.

[29] Y. Law, J. Doumen, and P. Hartel. Survey and benchmark of block ciphers for Wireless sensor networks. Tech. Rep. TRCTIT-04-07, Centre for Telematics and Information Technology, University of Twente, The Netherlands, 2004.

[30] N. Gura, A. Patel, A. Wander, H. Eberle, and S. Shantz. Comparing elliptic curve cryptography and rsa on 8bit cpus. In 2004 workshop on Cryptographic Hardware and Embedded Systems, Aug. 2004.

[31] Perrig, Culler,R. Szewczyk, D. 'I‘ygar, V. Wen, and D. "SPINS: Security protocols for sensor networks", Wireless Networks Journal (WINE), September 2002.

[32] Karlof, N. Sastry, and D. Wagner. TinySec: A Link Layer Security Architecture for Wireless Sensor Networks. Proceedings of the 2nd international conference on Embedded networked sensor systems, pp 162-175, November 2004.

[33] D. Wood and J. A. Stankovic, Denial of service in Sensor networks, computerm Vol. 35, no. 10, pp. 54-62, 2002.

[34] D. Wood and J . A. Stankovic. Denial of service in sensor networks. Computer, 35(10):54-62, 2002.

[35] Karp and H. T. Kung,“GPSR: greedy perimeter stateless routing for wireless networks,” in Mobile Computing and Networking, 2000, pp. 243-254.

[36] Y.-C. Hu, A. Perrig, and D. B. Johnson, “Wormhole detection in wireless ad hoc networks,” Department of Computer Science, Rice University, Tech. Rep. TR01-384, June 2002.

[37] J . R. Douceur, The Sybil Attack, in lst International Workshop on Peer-to-Peer Systems (IPTPS 02), March 2002.

[38] S. Avancha, J . Undercoffer, A. Joshi, and J . Pinkston, “Secure sensor networks for perimeter protection,” Computer Networks Wireless Sensor Networks, vol. 43, no. 4, pp. 421-435, 2003.

[39] Intanagonwiwat, R. Govindan, D. Estrin, JHeidemann, F. Silva, "Directed Diffusion for Wireless Sensor

©2021 The Author(s). Published by Infogain Publication.
This work is licensed under a Creative Commons Attribution 4.0 License. http://creativecommons.org/licenses/by/4.0/

[40] N. Shrivastava, C. Buragohain, D. Agrawal, and S. Suri. Medians and beyond: new aggregation techniques for sensor networks. In SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems, pages 239249. ACM Press, 2004.

[41] L. Hu and D. Evans, "Secure aggregation for wireless networks", Proc. of Workshop on Security and Assurance in Ad hoc Networks, Jan 28, Orlando, FL, 2003.

[42] R. C. Merkle, "Protocols for public key cryptosystems", Proc. of the IEEE Symposium on Research in Security and Privacy, April 1980, pp. 122134.

[43] [50].W. Du and J. Deng and Y. S. Han and P. K.' Varshney, "A Witness-Based :Approach for Data Fusion Assurance in Wireless Sensor Networks", in Proc. of IEEE Global Telecommunications Conference (GLOBECOM '03), pp. 1435-92003.

[44] K. Wu, D. Dreef, B. Sun, and Y. Xiao, "Secure Data Aggregation without Persistent Cryptographic Operations in Wireless Sensor Networks", Proc. of 25th IEEE International Pe@ormance, Computing, and Communications Conference. (IPCCC) 2006. , pp. 635-640,2006.

[45] [52]. Donggang Liu and Peng Ning, "Establishing pairwise keys in distributed sensor networks," in Proceedings of ACM CCS, October 2003.

[46] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," in Proceedings of ACM CCS, October 2003.

[47] W. Zhang, H. Song, S. Zhu, and G. Cao, "Least Privilege and Privilege Deprivation: Towards Tolerating Mobile Sink Compromises in Wireless Sensor Networks," ACM MobiHoc, May 2005.

[48] M. Hawkins, Identification of Outliers, New York: Chapman and Hall, 1980. [561.Rosner, "Percentage points for generalized esd many-outlier procedure," Technometrics, 1983.

[49] [57].J. E. Seem, G. Wi, Method of Intelligent data Analysis to Detect Abnormal Use of Utilities in Buildings, US patents, Patent no. US6816811 B2, Nov 2004.

[50] H. Song, S. Zhu, G. Cao, Attack-resilient time synchronization for Wireless sensor networks, in IEEE MASS, 2005, pp765-772.

[51] Y. Sun, W. Yu, and K. Riu. Trust Modelling and Evaluation for Ad Hoc Networks, GLOBECOM IEEE, Dec, 2005.

[52] Becher, Z. Benenson, and M. Dornseif. Tampering with motes: Real-world physical attacks on wireless sensor networks. In 3rd International Conference on Security in Pervasive Computing (SPC), April 2006.

[53] Wagner, Resilient Aaggregation in Sensor Networks, Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, 2004

[54] Z. Liang and W. Shi. PET: A P Ersonalized Trust model with reputation and risk evaluation for P2P resource sharing. Proceedings of the HICSS-38, Jan. 2005.

[55] S. Slijepsevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck, and M. Srivastava, "On communication security in wireless adhoc sensor networks," in Proc. 11th IEEE Int. Workshops Enabling Technol.: Infrastructure for Collaborative Enterprises, Jun. 2002.

[56] B. Przydatek, D. Song, and A. Perrig, "SIA: Secure information aggregation in sensor networks", Proc. of SenSys'03, Nov 5-7, Los Angeles, CA, 2003.

[57] J. Deng, R. Han, and S. Mishra. Countermeasuers against trafTic analysis in wireless sensor networks. Technical Report CU-CS-987-04, University of Colorado at Boulder, 2004.

©2021 The Author(s). Published by Infogain Publication.
This work is licensed under a Creative Commons Attribution 4.0 License. http://creativecommons.org/licenses/by/4.0/