Survey on Energy-Efficient Secure Routing In Wireless Sensor Networks

Venkatesh Shankar[1] Dr Rajashree V Biradar[2]
CSE Dept SITCOE, Yadrav, India
CSE Dept BITM, Bellary, India

ABSTRACT

Data security and energy aware communication are key aspects in design of modern ad-hoc networks. In this paper we investigate issues associated with the development of secure IEEE 802.15.4 based wireless sensor networks (WSNs) – a special type of ad hoc networks. We focus on energy aware security architectures and protocols for use in WSNs. To give the motivation behind energy efficient secure networks, first, the security requirements of wireless sensor networks are presented and the relationships between network security and network lifetime limited by often in-sufficient resources of network nodes are explained. Second, a short literature survey of energy aware security solutions for use in WSNs is presented.

KEYWORDS: *energy aware security architectures, routing protocols, security protocols, wireless sensor networks, WSN.*

I. INTRODUCTION

Wireless Sensor Networks have emerged as an important new area in wireless technology. In the near future, the wireless sensor networks are expected to consist of thousands of inexpensive nodes, each having sensing capability with limited computational and communication power [1] , [2] and [3] which enable us to deploy a large-scale sensor network.A wireless network consisting of tiny devices which monitor physical or environmental conditions such as temperature, pressure, motion or pollutants etc. at different areas. Such sensor networks are expected to be widely deployed in a vast variety of environments for commercial, civil, and military applications such as surveillance, vehicle tracking, climate and habitat monitoring, intelligence, medical, and acoustic data gathering. The key limitations of wireless sensor networks are the storage, power and processing. These limitations and the specific architecture of sensor nodes call for energy efficient and secure communication protocols.Normally sensor nodes are spatially distributed throughout the region which has to be monitored they self-organize in to a network through wireless communication and collaborate with each other to accomplish the common task. Basic features of sensor networks are self-organizing capabilities, dynamic network topology, limited power, node failures and mobility of nodes, short-range broadcast communication and multi-hop routing, and large scale of deployment [4]. The strength of wireless sensor network lies in their flexibility and scalability. The capability of self-organize and wireless communication made them to be deployed in an ad-hoc fashion in remote or hazardous location without the need of any existing infrastructure. Through multi-hop communication a sensor node can communicate a far away node in the network. This allows the addition of sensor nodes in the network to expand the monitored area and hence proves its scalability and flexibility property.

The key challenge in sensor networks is to maximize the lifetime of sensor nodes due to the fact that it is not feasible to replace the batteries of thousands of sensor nodes. Therefore, computational operations of nodes and communication protocols must be made as energy efficient as possible. Among these protocols data transmission protocols have much more importance in terms of energy, since the energy required for data transmission takes 70 % of the total energy consumption of a wireless sensor network Area coverage and data aggregation techniques can greatly help conserve the scarce energy resources by eliminating data redundancy and minimizing the number of data transmissions. Therefore, data aggregation methods in sensor networks are extensively investigated in the literature [4], [5], [6] and [7].

Security in data communication is another important issue to be considered while designing wireless sensor networks, as wireless sensor networks may be deployed in hostile areas such as battle fields. Therefore, data aggregation protocols should work with the data communication security protocols, as any conflict between these protocols might create loopholes in network security.

II. SENSOR NETWORK CHALLENGES

Wireless sensor network uses a wide variety of application and to impact these applications in real world environments, we need more efficient protocols and algorithms. Designing a new protocol or algorithm address some challenges are summarized below

2.1 Physical Resource Constraints:

The most important constraint imposed on sensor network is the limited battery power of sensor nodes. The effective lifetime of a sensor node is directly determined by its power supply. Hence lifetime of a sensor network is also determined by the power supply. Hence the energy consumption is main design issue of a protocol. Limited Computational power and memory size is another constraint that affects the amount of data that can be stored in individual sensor nodes. So the protocol should be simple and light-weighted. Communication delay in sensor network can be high due to limited communication channel shared by all nodes within each other's transmission range.

2.2 Ad-hoc Deployment:

Many applications are requires the ad-hoc deployment of sensor nodes in the specific area. Sensor nodes are randomly deployed over the region without any infrastructure and prior knowledge of topology. In such a situation, it is up to the nodes to identify its connectivity and distribution between the nodes. As an example, for event detection in a battle field the nodes typically would be dropped in to the enemy area from a plane.

2.3 Fault-Tolerance:

In a hostile environment, a sensor node may fail due to physical damage or lack of energy (power). If some nodes fail, the protocols that are working upon must accommodate these changes in the network. As an example, for routing or aggregation protocol, they must find suitable paths or aggregation point in case of these kinds of failures.

2.4 Scalability:

Most of the applications are needed the number of sensor nodes deployed must be in order of hundreds, thousands or more. The protocols must scalable enough to respond and operate with such large number of sensor nodes.

2.5 Quality of Service:

Some real time sensor application is very time critical which means the data should be delivered within a certain period of time from the moment it is sensed otherwise the data will be unusable So this must be a QOS parameter for some applications.

2.6 Security:

Security is very critical parameter in sensor networks, given some of the proposed applications. An effective compromise must be obtained between the low bandwidth requirements of sensor network applications and security demands for secure data communication in the sensor networks (which traditionally place considerable strain on resources)Thus, unlike traditional networks, where the focus is on maximizing channel throughput with secure transmission.

III. SECURITY REQUIREMENTS OF WSN

Security for wireless sensor networks should focus on the protection of the data itself and the network connections between the nodes [8]–[10]. In general, security requirements often vary with application. In WSNs we can distinguish the following important requirements of security capabilities, authentication and authorization, availability, confidentiality, integrity and freshness. Thus, we need some mechanism for access authorization and protecting a mobile code. In many applications we need to protect fair access to communication channels and at the same time we often need to hide the information about physical location of our sensor node. Moreover, we need to secure routing and we have to defend our network against denial of service, malicious flows, node capturing and node injection, etc.

3.1 Authorization.

Data authorization specifies access rights to resources and is strongly related to access control. Access control should prevent unauthorized users from participating in network resources. Hence, only authorized users can join a given network. Access control relies on access policies that are formalized, like access control rules in a computer system. Most modern operating systems include access control.

3.2 Authentication.

Message authentication implies a sender verification using cryptographic key. Authentication mechanisms are used to detect maliciously or spoofed packets. They are especially important in WSNs which use a shared wireless medium. In case of unicast transmission, an authentication can be guaranteed by symmetric key cryptography, using Message Authentication Code (MAC) .

3.3 Availability.

In secure network data should be safe and accessible at all times. Availability guarantees the survivability of network services against Denial-of-Service (DoS) attacks that can be launched at any layer of a wireless sensor network, and may disable a given device (network node) permanently. Moreover, DoS attack involved excessive computation and communication may exhaust battery charge of a sensor device.

3.4 Confidentiality.

In WSN keeping sensitive data secret is the most important issue in case of critical applications in which highly sensitive data (secret keys, sensitive measurements, etc.) are collected and transmitted. Data confidentiality ensures that sensitive data is never disclosed to unauthorized users or entities. Hence, measurement data should not be available to neighboring nodes, and secure channels between nodes should be created. To protect a network against cyber attacks and malicious nodes, the routing information and sensor identities should remain confidential too. The standard approach to prevent end-to-end data confidentiality is to encrypt the data with a secret key.

3.5 Integrity and freshness

Data integrity is the quality of correctness, completeness, wholeness, soundness and compliance with the intention of the creators of the data. It is achieved by preventing unauthorized insertion, modification or destruction of data. In WSNs a malicious node may change messages to perturb the network functionality. Moreover, due to unreliable communication channels it is easy to inject infected packets or alerted data. In WSNs data integrity guarantees that a message being transferred is never corrupted, but providing data integrity is not enough for wireless communication. The compromised sensor nodes can listen to transmitted messages and replay attacks. Data freshness protects data against replay attacks by ensuring that the transmitted data is recent one.

IV. ENERGY EFFICIENT SECURITY ARCHITECTURES AND PROTOCOLS

4.1 SERP: Secure Energy Efficient Routing Protocol

The secure energy efficient routing protocol for wireless sensor networks (SERP) is described in [11]. The main idea of this protocol is to provide a robust transmission of authenticated and confidential data from the source sensor with limited energy budget to the base station. It is dedicated to WSNs with densely deployed relatively static sensor devices.

Three main objectives were considered during design of SERP:

- Energy aware organization of the network to ensure energy efficient transmission, and finally maximum lifetime of the network,
- Secure transmission: nodes should have the capability to detect falsely injected reports,
- Robust and resilient transmission: any node failure would not greatly hamper the performance of a network.

The protocol operates in two main phases: creating a back bone network and secure data transmission. A sink rooted tree structure is created as the backbone of the network taking into consideration balanced energy consumption. Next, a minimum number of forwarding nodes in the network is selected. The backbone network is restructured periodically. It is used for authenticated and encrypted data delivery from the source sensors to the base station. A one way hash chain and pre-stored shared secret keys are used for ensuring secure data transmission. An optional key refreshment mechanism that could be applied depending on the application is introduced for data freshness. The energy saving mechanism is based on disable the radio transceivers of selected nodes. The nodes in a network can operate in two main states *non-forwarding* – the transceiver is switched off, *forwarding* – both transceiver and sensing devices are switched on. It is assumed that after the backbone structure is constructed all nodes are either in forwarding or non-forwarding states.

4.2 EENC: Energy Efficiency Routing with Node Compromised Resistance

A novel energy efficiency routing protocol with node com- promised resistance (EENC) was developed by K. Lin *et al.*, and described in [12]. EENC bypasses the compromised nodes and improves the accuracy of packets under the condition of balancing the energy consumption. The Reinforcement learning based on the ant

Architecture	Security services	Properties
SPINS	Authentication, authenticated broadcast, confidentiality, integrity, freshness.	Consists of SNEP and µTesla (secure building blocks). Symmetric cryptography support. Encryption (CTR mode), Block Cipher (RC5). Not fully implemented and specified.
TinySec Authentication	Authentication, confidentiality, integrity, replay protection	Link layer architecture easily integrated into WSN. Symmetric cryptography support.

Table 1 : Summary of selected security architectures for WSN

colony optimization is used to complete routing tables. The trust values are assigned to all nodes of a network. The trust value is computed and based on the multiple behavior attributes such as packet drop rate, forwarding delay rate, etc. These values are used to detect the malicious nodes. Each node in a WSN computes the trust values of its one hop neighbors. The idea of EENC was to provide security with minimal energy consumption. To achieve this, each node storages trust values of all its neighbors and manages its energy resources.The EENC protocol operates as follows. To transmit data the secure and energy efficient route is computed. The calculation process consists of many rounds, each divided into three phases.• Routing detecting phase. A certain number of forward ants are generated to search for route leading to the sink. Each ant records the information about the minimum amount of energy and minimum trust value for nodes along the path, and the hop number for each node. • Pheromone updating phase. The sink node generates a backward ant, which carries all data collected by the forward ant. These data are used to update the pheromone value concerned with each node in a path. • Routing maintaining phase. The route for a given source and sink nodes is established based on trust values and updated pheromone values of the nodes carried during the pheromone updating phase. The Table 1 presents the summary of our survey – security architectures, provided services and their main properties

4.3.Summary and Conclusions

Many challenges arise from application of wireless ad hoc networking. We focused on one of them that is very important in wireless sensor networks – secure data protection and data transmission in WSN with limited resources. The paper provides a short overview of some representative energy efficient security techniques. We briefly discussed the security requirements of WSNs and showed the relationships between techniques for forming secure networks, and energy aware WSNs. Next, we described and compared based on literature survey selected energy aware architectures and protocols in WSNs that can be implemented in the physical, data link, network, and middleware layers of the OSI model.In summary, we can say that due to scarce resources, unique properties of wireless sensor networks, and often hostile environments it is a challenging task to protect sensitive information transmitted by nodes forming a WSN. Due to limited resources of nodes that form WSN many solutions providing strong security are impractical in this type of network. Therefore, we can find many security considerations that should be investigated in the nearest future.

REFERENCES

[1]. W. Su Y. Sankarasubramaniam E. Cayirci Akyildiz, I.F. A survey on sensor networks. *IEEE Communications Magazine*, 2002.

[2]. Kumar.S.P. Chee-Yee Chong. Sensor networks: Evolution, opportunities, and challenges. *Proc IEEE*, August 2003.

[3]. Ismail H. Kasimoglui Ian .F. Akyildiz. Wireless sensor and actor research challenges. *(Elsevier) Journal*, 2004.

[4]. D. Agrawal N. Shrivastava, C. Buragohain and S. Suri. Medians and beyond: new aggregation techniques for sensor networks. *Proceedings of the 2nd inter- national conference on Embedded networked sensor systems*, 2004. ACM Press.

[5]. Xiuli Ren and Haibin Yu1. Security mechanisms for wireless sensor networks. *IJCSNS International Journal of Computer Science and Network Security*, VOL.6(No.3):100-107, March 2006.

[6]. S. Setia S. Zhu and S. Jajodia. Leap: e±cient security mechanisms for large scale distributed sensor networks. *Proceedings of the 10th ACM conference on Computer and communications security*, 2003. ACM Press.

[7] P.Nair H.Cam, S.Ozdemir and D. Muthuavinashiappan. Espda Energy - efficient and secure pattern based data aggregation for wireless sensor networks. *Computer Communications IEEE Sensors*, 2006.

[8] M. Ahmad, M. Habib, and J. Muhammad, "Analysis of security protocols for Wireless Sensor Networks", in *Proc. 3rd Int. Conf. Comp. Res. Develop. ICCRD 2011*, Shanghai, China, 2011, vol. 2, pp. 383–387.

[9] C. Castelluccia, A. C.-F. Chan, E. Mykletun, and G. Tsudik, "Efficient and provably secure aggregation of encrypted data in wireless sensor networks", *J. ACM Trans. Sensor Netw. (TOSN)*, vol. 5, no. 3, 2009.

[10] S. R. Gandham, M. Dawande, R. Prakash, and S. Venkatesan, S., *Energy efficient schemes for wireless sensor networks with multiple mobile base stations*, in *Proc. IEEE Global Telecom. Conf. GLOBE- COM'03*, San Francisco, USA, 2003, vol. 1, pp. 377–381.

[11] A. K. Pathan and C. S. Hong, "SERP: secure energy-efficient routing protocol for densely deployed wireless sensor network", *Annales des Telecomm.*, pp. 529–541, 2008.

[12] K. Lin, Ch. F. Lai, X. Liu, and X. Guan, "Energy efficiency routing with node compromised resistance in wireless sensor networks", *Mob. Netw. Appl.*, vol. 17, pp. 75–89, 2012.