ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

An Innovative and Secure On-Demand Routing Protocol for Wireless Sensor Network

Agnibha De
B. Tech in Electrical Engineering,
M. Tech in Computer Science and Engineering.

Abstract

Popularity of wireless sensor nowadays is something pervasive and the examples are ample where this technology is being used e.g. military system, home security, hospitals, sales support, tracking application etc. Though the major flaw of the network topology of such applications is that, the sensor nodes which are used, are made exposed to several attacks and thus are vulnerable. The vulnerabilities are many like - wormhole, replication and sinkhole attack. Therefore, though this network infrastructure is backbone for many applications, the requirement of more robust architecture in terms of security is a need of time. More specifically, designing an algorithm which not only take care the potential network attacks but also become energy efficient is what we can call innovative here. In this paper, a secure routing and aggregation protocol (STAPLE) which is highly energy efficient at the same time is discussed and is presented.

Introduction

The primary reasons behind the emergence of wireless sensor network nowadays are firstly its being cheap and also having a singular point of control for a vast range of different scenario. Additionally, the very recent developments of IEEE 802.15.4 has fueled the significance of wireless sensor network. These developments include formalization of ZigBee standard which operate at application and network layer. The traditional security measures seem inapplicable for the wireless sensor network owing to the limited resources at the intermediate sensor nodes. Being so, the sensor networks are vulnerable to many types of penetrations like Sinkhole, Replication Attack, Man in the Middle etc. To prevent these systems from remaining open to such vulnerabilities, a number of secure routing protocol has come into place. STAPLE may be considered as one of such protocols which is mentionable due to its consuming lowest energy. The security measures employed by this routing protocol is by utilization of one directional hashing and multi-path routing through which it ensures non-repudiation and data integrity. The working of STAPLE may be described into the following three stages:

a) Initialization
b) Transmission
c) Authentication of Source

We will discuss these stages sequentially:

a) Initialization- Depending upon the distributing key and sink node, at initial phase, different nodes are arranged at different levels.

b) Transmission- In this transmission phase, STAPLE algorithm deals with the task of forwarding the data packets from child nodes to parent nodes until they packets reach the sink node concerned while maintaining child node authentication and data integrity.

c) Authentication of Source – This is the last stage which involves checking the authenticity of the source where the data packets are said to be delivered.

Associated Functioning

a) Omni-directional Hash Chain

Hash chain is the cryptographic tool in order to generate multiple keys or password from a single key. This is like other cryptographic methods but having a different method of generation of the keys. Such kind of hashing is very useful for sensor network topography since the situations are most likely met where the sensors happen to be constrained by resource utilization.

b) Routing Protocols

Ad Hoc routing protocols are found to be most suitable for Wireless Sensor Network where algorithm works primarily on On-Demand basis. DSRP (Dynamic Source Routing Protocol) is one of such protocols which functions on restricted bandwidth while control packets are transmitted with the use of routing table which updates periodically with proactive messaging within the network. The major difference between DSRP and any other on demand Ad Hoc Routing Protocol (Wireless) is that in case of DSRP, there is no need of periodic transmission of Hello Packets (and thus it is beacon-less) which is disseminated from the

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

sink node to its neighboring nodes to advertise its existence.

Within our network topography, each of the nodes are found to comprise of several information which can be found as follows:

Sensor node parameters

Information of nod	Description
Id	The unique integer in network allocated to a sensor node
Level	The minimum number of hops away from the sink node
Key	A node has a one or more keys, generated by its parent keys, with HMAC functions. They are utilized to encrypt data & authenticate children's identity
MAC	A node has only one MAC, generated by its own ID with HMCA functions. It is utilized to authenticate source node's identity
Parents	A node's neighboring node in the previous level
Brothers	A node's neighboring node in the same level
Children	A node's neighboring node in the previous level

For illustration, it may be considered that in a certain topography of network configuration, there are a number of sinks and b number of sensors present. In the current discourse, these sensor nodes will be divided into a number of clusters which will contain a single sink within it and b/a number of sensor nodes.

Working of staple

a) **Initialization of Network:**
The initialization work of STAPLE algorithm operates based on the activity of the sink node which organize the rest of the nodes, i.e. sensor nodes in different layers based on the lowest number of hops in terms of the sink node itself. Consequently the keys and the MACs are generated aiming to build the hash chain. The function of Initialization may be summarized down as:

- Discover and organize all the nodes with their corresponding distances.
- Generate Cryptographic key and MAC for each organized nodes.

b) Transmission of Data and Filtering:
The transmission of the data takes place from the initial node, which then transmit the same to its parent node and the transmission pattern follows the same schema. Also, the packets are authenticated in the intermediate nodes in the course of its transit time. The functioning of this phase may be summarized as:

- Authenticating the identity of the child node
- Maintaining the Data Integrity
- Scanning and Filtering wrong data packets

c) Source Authentication in Sink:
In this last phase of the process, the data packets are authenticated at the sink node upon arrival. Also, the data integrity is maintained in this case. Hence, the functioning at this phase may be summarized as:

- Authenticating the identity of the source node
- Maintaining and Assuring the Data Integrity

Conclusion

Due to recent advancement in the field of wireless sensor networking, a lot of unforeseen problems cropped up, particularly from the perspective of security which was not familiar to the security for traditional routing in case of wired communication. As a solution, a number of efficient algorithms are found to be prevalent and in this paper, we have discussed the routing protocol termed as STAPLE which is based on on-demand Ad Hoc routing protocol.

Routing in sensor networks has attracted a lot of attention in the recent years and introduced unique challenges compared to traditional data routing in wired networks. In this paper a secure routing protocol named STAPLE is discussed. The security is achieved by one way hash chain and multi path routing mechanism. The routing protocols that use multi sink, routing protocols are deployed only a single sink. Implementing these protocol and technologies into routing protocols introduces security holes that should not be compromised.

References

[1] *D. Culler, "Secure, low-power, IP-based connectivity with IEEE 802.15.4 wireless networks," Industrial Embedded Systems, 2007.*

[2] *Z. Alliance, Zigbee alliance, http://www.zigbee.org.*

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

[4] *Y. Yang, X. Wang, S. Zhu, and G. Cao, "Sdap: a secure hop-by-hop data aggregation protocol for sensor networks," in MobiHoc, 2006, pp. 356–367.*

[5] *R. C. Merkle, "A certified digital signature," in CRYPTO, 1989, pp. 218–238*

[6] *http://markus-jakobsson.com/papers/jakobsson-acns05.pdf*

[7] *AlyMohamed El-Semary and Mohamed Mostafa Abdel-Azim: "New Trends in Secure Routing Protocols for Wireless Sensor Networks" in Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2013, Article ID 802526,*

[8] *en.wikipedia.org/wiki*

[9] *H. Chan and A. Perrig, "Security and privacy in sensor networks," IEEE Computer, vol. 36, no. 10, pp. 103–105, 2003.*

[10] *[A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," IEEE Computer, vol. 35, no. 10, pp. 54–62, 2002.*