Data Security in WSN based on Location

C.Rajagopal
Asst prof(SG)/IT
Saveetha school of Engineering

V.Ajitha
Asst prof(SG)CSE,
Saveetha Engineering College

Abstract— The targeted terrain is virtually divided into multiple cells using a concept called virtual geographic grid. Then it efficiently binds the location (cell) information of each sensor into all types of symmetric secret keys owned by that node. By this means, the impact of compromised nodes can be effectively confined to their vicinity, which is a nice property absent in most existing security designs. What the attacker can do is to misbehave only at the locations of compromised nodes, by which they will run a high risk of being detected by legitimate nodes if effective misbehavior detection mechanisms are implemented. Proposed system provides end-to-end security guarantee. Every legitimate event report is endorsed by multiple sensing nodes and is encrypted with a unique secret key shared between the event sensing nodes and the sink. Furthermore, the authenticity of the corresponding event sensing nodes can be individually verified by the sink. This novel setting successfully eliminates the possibility that the compromise of nodes other than the sensing nodes of an event report may result in security compromise of that event report, which is usually the case in existing security designs. Proposed system possesses efficient en-route false data filtering capability to deal with the infamous bogus data injection attack.

Keywords— Virtual Geographic Grid, End-to-End Security, Data Filtering,Compromised node,attacker

I. INTRODUCTION

Wireless sensor networks (WSNs) have attracted a lot of attention recently due to their broad applications in both military and civilian operations. WSNs usually consist of a large number of ultra small low-cost battery-powered devices that have limited energy resources, computation, memory, and communication capacities and according to different applications such as battlefield reconnaissance and homeland security monitoring, WSNs are often deployed in a vast terrain to detect events of interest and deliver data reports over multihop wireless paths to the sink. Data security is essential for these mission-critical applications to work in unattended and even hostile environments. One of the most severe security threats in WSNs is security compromise of sensor nodes due to their lack of tamper resistance. In WSNs, the attacker could compromise multiple nodes to obtain their carried keying materials and control them and thus is able to intercept data transmitted through these nodes thereafter. As the number of compromised nodes grows, communication links between uncompromised nodes might also be compromised through malicious cryptanalysis. Hence, this type of attack could lead to severe data confidentiality compromise in WSNs. Furthermore, the attacker may use compromised nodes to inject bogus data traffic in WSNs. In such attacks, compromised nodes pretend to have detected an event of interest within their vicinity or simply fabricate a bogus event report claiming a non existing event at an arbitrary location. Such insider attacks can severely damage network function and result in the failure of mission-critical applications. This paper aims to overcome these problems and to transfer the data providing confidentiality, authenticity and availability. It should be robust against attacks.

II. RELATED WORK

Existing security designs provide a hop-by-hop security paradigm only, which leaves the end-to-end data security at high stake. Data confidentiality and authenticity is highly vulnerable to insider attacks, and the multihop transmission of messages aggravates the situation. Moreover, data availability is not sufficiently addressed in existing security designs, many of which are highly vulnerable to many types of Denial of Service (DoS) attacks.

Limitations:

The requirements of data security in WSNs are basically the same as those well defined in the traditional networks, that is, data confidentiality, authenticity, and availability. Data should be accessible only to authorized entities (usually the sink in WSNs), should be genuine, and should be always available upon request to the authorized entities.In the past few years, many secret key predistribution schemes have been proposed. By leveraging preloaded

keying materials on each sensor node, these schemes establish pairwise keys between a node and its neighbors after network deployment for every network node, respectively, and thus form a hop-by hop security paradigm

III. SYSTEM ARCHITECTURE

The architecture explains how the data is transmitting from home cell to destination cell (sink cell) through intermediate cells. Each cell has its corresponding sensor. The sensor will have communication with all the nodes in the cells. It collects the report and check its authentication and to the corresponding transmission to cells/nodes.
Level 1 : Data transmission

Level 2 : Encryption and Decryption of data

Level 3 : Key sharing

Level 4 : Involvement of Home and Sink sensor.

IV. IMPLEMENTATION

4.1 LOCATION AWARE KEY MANAGEMENT FRAMEWORK

Before network deployment, the network planner prepares a geographic virtual grid of the targeted terrain with reference point and cell size l. Based on the total number of nodes in the network N, cell size l, and the average number of nodes in each cell n0, the network planner further decides the values of T and t: The former is the number of endorsements included when generating a valid report, and the latter defines the minimum number of correct endorsements to validate a report.
Report-forward route: An event report is relayed from the event cell to the sink in a cell-by-cell basis along its report-forward route. A report is always relayed between adjacent cells toward the sink.

4.2 END - TO - END DATA SECURITY

Proposed system requires each valid event report to be encrypted and, at the same time, attached with T endorsements from T different nodes when generated from the event cell. Although an event report is relayed to the sink, the intermediate nodes will drop any invalid endorsements to the report. Moreover, the report itself will be dropped when the number of valid endorsements becomes less than t. This is in contrast to the existing designs in which a report is dropped as soon as an invalid endorsement is found.
The proposed design is important as it makes the system more robust in that it tolerates up to T-t compromised nodes in an event cell colluding to launch a report disruption attack by contributing invalid endorsements to the legal event reports. Meanwhile, the requirement of multiple endorsements makes the system more reliable by disabling the possibility that up to t-1 compromised nodes of an event cell or an unlimited number of compromised nodes from any other cell(s) collude to forge a report of events “appearing” at that event cell. The encryption prevents an unlimited number of compromised nodes not in the event cell from colluding to obtain the content of the reports. LEDS further adopts a one-to-many report-forwarding paradigm, which ensures that the system is being highly resilient to selective message forward attacks.
The final report contains

- An event cell id,
- The ids of T participating nodes,
- A C share
- T + 1 MACs

4.3 DATA FILTERING

In proposed system, data reports are relayed cell by cell and delivered following a robust one to many, instead of existing failure-prone one-to one forwarding paradigm. A sending/intermediate node locally broadcasts a data report to the next cell in its route forward route. As we mentioned before, it is easy to determine the next cell on the report-forward route, which is the one that is adjacent to the sending cell and is closer to the sink. Nodes in the receiving cell verify the report, and upon successful verification and processing, one of them rebroadcasts the report further to the next cell. Again, duplicate reports are suppressed by using the techniques like back off before sending.

In proposed system, an appropriate intermediate node authenticates a received report by checking 1) the validity of the first MAC attached in the report and 2) the number of nonzero Macs. The node verifies the first MAC attached in the report by using the corresponding authentication key:

- If the first MAC is zero, it deletes it and attaches another zero to the next to the end of the report.4
- If the first MAC is valid, it deletes it and attaches a new MAC to the next to the end of the report.
- If the first MAC is invalid, it deletes it and attaches a zero to the next to the end of the report.

V. ALGORITHM DESCRIPTION

5.1 IDEA ALGORITHM:

IDEA is:

- Strong, small, and fast
- Resistant against known crypto attacks
- Available worldwide
- Offers patent protection against fraud and piracy

IDEA is the name of a proven, secure, and universally applicable block encryption algorithm, which permits effective protection of transmitted and stored data against unauthorized access by third parties. The fundamental criteria for the development of IDEA were highest security requirements along with easy hardware and software implementation for fast execution.Benefits of the IDEA encryption algorithm

- provides high level security not based on keeping the algorithm a secret, but rather upon ignorance of the secret key
- is fully specified and easily understood
- is available to everybody
- is suitable for use in a wide range of applications
- can be economically implemented in electronic components
- can be used efficiently
- may be exported world wide
- is patent protected to prevent fraud and piracy

5.2 Description of the algorithm

The block cipher algorithm IDEA™ operates with 64-bit plain text and cipher text blocks and is controlled by a 128-bit key. The fundamental innovation in the design of this algorithm is the use of operations from three different algebraic groups. The substitution boxes and the associated "table lookups" used in the block cipher available to-date (amongst them DES) have been completely dispensed with.

The algorithm structure has been chosen such that, with the exception that different key sub-blocks are used, the encryption process consists of eight identical encryption steps (known as encryption rounds) followed by an output transformation. The structure of the first round is shown in detail. The 64-bit plain text block is partitioned into four 16-bit sub-blocks, since all the algebraic operations used in the encryption process operate on 16-bit numbers. Another process, which is described below, produces for each of the encryption rounds, six 16-bit key sub-blocks from the 128-bit key. Since a further four 16-bit key sub-blocks are required for the subsequent output transformation, a total of 52 (= 8 x 6 + 4) different 16-bit sub-blocks have to be generated from the 128-bit key. In the first encryption round, the first four 16-bit key sub-blocks are combined with two of the 16-bit plain text blocks using addition modulo 2 ˆ(16), and with the other two of the 16-bit plain text blocks using multiplication modulo 2ˆ(16 +1).

The results are then processed further as shown in the flowchart. Whereby two more 16-bit key sub-blocks enter the calculation and the third algebraic group operator, the bit-by-bit exclusive OR, is used. At the end of the first

encryption round four 16-bit values are produced which are used as input to the second encryption round in a partially changed order.
The process described above for sound one is repeated in each of the subsequent 7 encryption rounds using different 16-bit key sub-blocks for each combination. During the subsequent output transformation, the four 16-bit values produces at the end of the 8th encryption round are combined with the last four of the 52 key sub-blocks using addition modulo 2ˆ16 and multiplication modulo 2ˆ(16 +1) to form the resulting four 16-bit cipher text blocks. It should be noted that at no point in the encryption process is the same algebraic group operation used contiguously. A special feature of the multiplication of two 16-bit sub-blocks modulo 2ˆ(16 +1), is that a 16-bit sub-block which consists of all 0 bits, is not interpreted as 0 but rather as 2ˆ16.

5.3 Decryption

The computational process used for decryption of the cipher text is essentially the same as that used for encryption of the plain text and hence the computational graph in the diagram is also valid here. The only difference compared with encryption is that during decryption, different 16-bit key sub-blocks are generated. More precisely, each of the 52 16-bit key sub-blocks used for decryption is the inverse of the key sub-block used during encryption in respect of the applied algebraic group operation. Additionally, the key sub-blocks must be used in the reverse order during decryption in order to reverse the encryption process.

VI. CONCLUSION AND FUTURE ENHANCEMENT

CONCLUSION

We considered and evaluated the end -to - end data security provided based on location. The proposed system provides end-to-end security guarantee. Every legitimate event report is endorsed by multiple sensing nodes and is encrypted with a unique secret key shared between the event sensing nodes and the sink. It possesses efficient en-route false data filtering capability to deal with the infamous bogus data injection attack. It is robust against the Denial of Service attack i.e. the selective forwarding attack and the report disruption attack.

FUTURE ENHANCEMENT

In this paper, the trustworthy of the nodes are selected randomly. We need some mechanism to find the trustworthy of the nodes. Trusted Distributed Authentication Model (DAM) is the future enhancement of this project. This concept is used to authenticate every node is trustworthy or not in particular cell. This concept is implementing in sensor nodes. The Trust management is based on a “Distributed Authentication Model” whose mechanism is trustworthiness acquiring and adjusting of network nodes with no online trusted servers. With this Distributed Authentication Model, protocol can exclude the attackers and selfish nodes timely and proactively.

REFERENCES

[1] A. Wood and J. Stankovic, “Denial of Service in Sensor Networks,” Computer, Oct. 2002.
[2] D. Liu and P. Ning, “Location-Based Pairwise Key Establishments for Relatively Static Sensor Networks,” Proc. ACM Workshop Security of Ad Hoc and Sensor Networks (SASN ’03), Oct. 2003
[3] D. Carman, P. Kruus, and B. Matt, “Constraints and Approaches for Distributed Sensor Network Security,” Technical Report 00010, NAI Labs, 2000.
[4] E. Shi and A. Perrig, “Designing Secure Sensor Networks,”Wireless Comm. Magazine, vol. 11, no. 6, Dec. 2004.
[5] F. Ye, H. Luo, S. Lu, and L. Zhang, “Statistical En-Route Filtering of Injected False Data in Sensor Networks,” Proc. IEEE INFOCOM, Mar. 2004.
[6] F. Ye, S. Lu, and L. Zhang, Gradient Broadcast: A Robust Data Delivery Protocol for Large Scale Sensor Networks, ACM/Baltzer J.Wireless Networks, Mar. 2005.
[7] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, “Toward Resilient Security in Wireless Sensor Networks,” Proc. ACM MobiHoc, 2005.
[8] H. Chan and A. Perrig, “Security and Privacy in Sensor Networks,” Computer, pp. 103-105, Oct. 2003.
[9] H. Chan, A. Perrig, and D. Song, “Random Key Predistribution Schemes for Sensor Networks,” Proc. IEEE Symp. Research in Security and Privacy, 2003.
[10] L. Eschenauer and V. Gligor, “A Key-Management Scheme for Distributed Sensor Networks,” Proc. Ninth ACM Conf. Computer and Comm. Security (CCS ’02), 2002.
[11] 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,” Proc. IEEE Symp. Security and Privacy, May 2004.
[12] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney, “A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge,” IEEE Trans. Dependable and Secure Computing, vol. 3, no. 2, pp. 62-77, Jan.-Mar. 2011.