Volume 4, Issue 11, November 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# An Effective Time Management Schema in WSNs

**Mulukalla Prasad**
Associate Professor in CSE
Scits, Karimnagar, India

**Varanganti Ravikumar**
Assistant Professor in CSE
Scce, Karimnagar, India

***Abstract- WSN usually consists of a large number of resource constraint sensor nodes that are generally deployed in unattended/hostile environments and Existing security designs mostly provide a hop-by-hop security paradigm. Furthermore, existing security designs are also vulnerable to many types of Denial of Service (DoS) attacks, such as random node capture attack, report disruption attacks and selective forwarding attacks. We come up with a new concept that provide end-to-end security framework in which secret keys are generated and each node stores a few keys based on Time Schema . The proposed multifunctional key management framework assures both node-to-sink and node-to-node authentication along the report forwarding routes.***

***Index Terms— Data security, wireless sensor network, end-to-end, DoS attack, false-data injection attack***

## I. INTRODUCTION

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 [1], [2], [4], [7], 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 [7]. 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. Hence, this type of attack could lead to severe data confidentiality, data availability and data authenticity [3], [5] in WSNs.

Due to the resource constraint, most of the proposals are based on symmetric cryptography and only provide data authenticity and/or confidentiality in a hop-by-hop manner. End-to-end encryption/ authentication is considered less feasible, particularly in a WSN consisting of a large number of nodes [7]. To make things worse, existing security designs are highly vulnerable to many types of Denial of Service (DoS) attacks such as report disruption attacks and selective forwarding attacksIn this paper, we propose an integrated security design providing comprehensive protection over data confidentiality, authenticity, and availability. Our design establishes a Time based end-to-end data security framework in WSNs.First, we propose a novel multifunctional key management framework using time constraint. In our concept, the targeted terrain is virtually divided into multiple cells using the concept of a virtual geographic gridSecond, it 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.Third, we possesses an efficient en-route false data filtering capability to deal with the infamous bogus data injection attack Last, it provides high-level assurance on data availability by dealing with both report disruption attack and selective forwarding attack [3] simultaneously

## II. BASIC KNOWLEDGE

### *A. End-to-End versus Hop-by-Hop Design*

In the past few years, the key distribution schema have been proposed [6], [8], [9], [10].The security strength of these schemes is analyzed in terms of the ratio of compromised communication links over total network communication links due to node compromise. Two types of node compromise are considered: random node capture and selective node capture, according to key distribution information available to the attacker. Hop-by-hop security design works fine when assuming a uniform wireless communication pattern in WSNs. in many applications, node-to-sink communication is the dominant communication pattern in WSNs, that is, data of interest are usually generated from the event happening area and transmitted all the way to the sink. In this case, hop-by-hop security design is not sufficient anymore as it is vulnerable to communication-pattern-oriented node capture attacks.

### *B. Existing Data Report Security Designs in WSNs*

The general approach is to protect the data Authenticity in WSNs is given as , to generate a valid report E nodes that sense the event should first agree on the content of the event report, and in order to be forwarded by intermediate nodes and accepted by the sink, a valid report should be collaboratively endorsed (usually through Message Authentication Codes (MACs)) by these T nodes. Once a node in a certain area is compromised, the attacker can disrupt any event report from that area from being forwarded to the sink thereafter by simply contributing a wrong MAC to the final report. As

 

the number of compromised nodes increases, the resulting damage will increase drastically, Hence, data availability , data confidentiality and data Authentication in these schemes is poorly assured. The Existing Systems are purely Based on Statistical en-route Filtering (SEF)[5] and Interleaved hop by Hop Authentication(IHA)[6]. The drawbacks of the above two schemas are solved and protect the data from DoS Attacks by Using Time Based Key Management Frame work.

## III. MECHANISM

### *A. System Assumptions.*

In this approach, we consider a large-scale uniformly distributed WSN that monitors a vast terrain of interest via a large number of static sensor nodes Once deployed, each node is assumed to be static and can obtain via a Time secure schema. We assume that every sensor node has a unique ID. We also assume that sensor nodes are not tamper resistant.

### *B. Threat Model*

We assume that if the node is compromised, all the information it holds will also be compromised We also assume that the attacker can eavesdrop on all traffic, inject packets, and replay older packets On the other hand, we assume that there is a short bootstrapping phase right after network deployment during which no sensor node is compromised.

### *C. Design Goals*

we focus on the data such as event reports that are generated by the sensing nodes and transmitted from the sensing area to the sink. The design of Time based Key Management is to achieve Provide end-to-end data confidentiality and authenticity and Achieve a high-level of assurance on data availability and Be resilient against report disruption attacks and selective forwarding attacks and be able to early detect and drop bogus reports in an effective and deterministic manner.

## IV. NOTATIONS AND TERMS

### *A. Home cell, event cell*

The parameters of a geographic virtual grid consist of a reference Time and the cell size. For convenience, the reference Time, referred to as $T_0$, is set to the sink, which is known before network deployment Home cell, event cell. The cell that a node, say, u, is located in after network deployment is called the home cell of u, denoted as $T_u$. We call a cell an event cell when a certain event of interest happens in that cell. Each report is therefore corresponding to one particular event cell.

### *B. 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. The report-forward route of node u therefore consists of all the cells that are intersected by the line segment that connects the center of $T_u$ and the sink.

### *C. Report-auth area*

The report-auth area of a node u consists of two parts, the downstream report-auth area and the upstream report-auth area. the downstream report-auth area of u is defined to be all the cells that are farther to the sink than $T_u$, and each has at least half a part located inside the sector area, whereas the upstream report auth area consists of all the cells that are closer to the sink than Iu and have any part that falls into the sector area.

## V. SCHEMA OVERVIEW

The proposed schema consists of two major components

### *A. Time management framework*

In this technique, each node stores three different types of keys: 1) A unique secret key shared between the node and the sink that is used to provide node-to-sink authentication.2) A cell key shared with other nodes in the same cell that is used to provide data confidentiality.

3) A set of authentication keys shared with the nodes in its report-auth cells that are used to provide both cell-to-cell authentication and en-route bogus data filtering.

### *B. End-to-end data security mechanism.*

*Data Confidentiality*: every event report is encrypted by the corresponding cell key of the event cell. The confidentiality of the report is guaranteed as long as no node in the event cell is compromised

*Data authenticity*: 1) Each report is endorsed by multiple sensing nodes, and the endorsements can be individually authenticated by the sink. 2) Each report is also authenticated in an interleaved cell-by-cell manner

*Data availability* The encrypted report is divided into a number of unique shares Each share is independently generated by a participating node using its unique secret key shared with sink.

Using cell-to-cell authentication keys guarantees that each report can be verified simultaneously by multiple next-hop nodes at any point in the route.

 

## VI. PROTOCOL DETAILS

### *A. Time Management Framework*

We assume that a group of mobile robots are dispatched to sweep across the whole sensor field along preplanned routes after the deployment of sensors The leading robot is also equipped with the following bootstrapping parameters:
$\{K^{I}_{M}, k^{II}m, l, T_0, E, e, P\}$
Where,
Reference Time: $T_0$ and cell size *l.*
Total number of nodes in the network N and the average number of nodes in each cell $n_0$,
E: The former is the number of endorsements included when generating a valid report
e: The minimum number of correct endorsements to validate a report
p: is a large Prime number.
First determine a node u's home cell $T_u$ and then compute a unique secret key $K_u = (H (K^{I}M \mid u \mid Tu))$
A cell key $K^{T}u = H (K^{I}M|T_u)$
The authentication key between the two adjacent cells is
$H (K^{II}_{M} \mid T_u \mid T_v))$

### *B. End to End Data Security Mechanism*

*a. Report generation*

Each of E participating nodes first agree on an event report M. M usually contains information such as event type, id of event cells, and a time stamp, etc. Note that all the related communications are protected by the cell key so that M is confidential against any outside node. Next, each participating node, say, u, encrypts M using the cell key $K_{Tu}$ and obtains $C = E_{KTu} (_M)$.

*b. Interleaved cell-by-cell en-route filtering*

A sending/intermediate node locally broadcasts a data report to the next cell in its route forward route 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. In this approach, 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.
- 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.

## VII. ALGORITHM

**Input:** Event Report
Cell Keys based on Time Constraints.
**Output:** Original Report with out any Interruption
**Method:**

```
Verify the 1st MAC Contained in the report
If (the 1st MAC is Zero or Invalid)
        new MAC = 0
If (the 1st MAC is valid)
        new MAC = createMAC (Key);
        delete the 1st MAC
        attach new MAC to the next to the end of the report
get number of different non zero MACs
if ((Num_of_MAC<E-j-2 || Num_of_MAC < e+1))
        discard report
else
        forward report to the next cell
```

Sink verifies
1) using the authentication keys it shares with the intermediate cells and checks and
2) by recovering the report C(cyper text) from $C_u$. To do this, it tries to recover C from any e correct shares and then decrypts the recovered C using the corresponding cell key of event cell. To do this, it tries to recover C from any e correct shares and then decrypts the recovered C using the corresponding cell key of event cell
The recovery operation of M goes as follows: sink picks e out of E shares, using their corresponding secret keys and sink further decrypts C and gets M. At this point, if M is meaningful (that is, conforming to the predefined report format), the recovery operation succeeds. Otherwise, sink tries another combination of t shares.

## VIII. RESULTS

### *A. Security Strength Regarding Data Confidentiality*

In fig 1, shows how the number of compromised nodes affects data confidentiality. It is clear that, to compromise 40 percent of the total cells, at least 5 percent of the total nodes have to be compromised. This means at least 500 nodes,

 

given N = 10;000 and n′ = 10. Furthermore, the security resilience increases as n′ decreases.

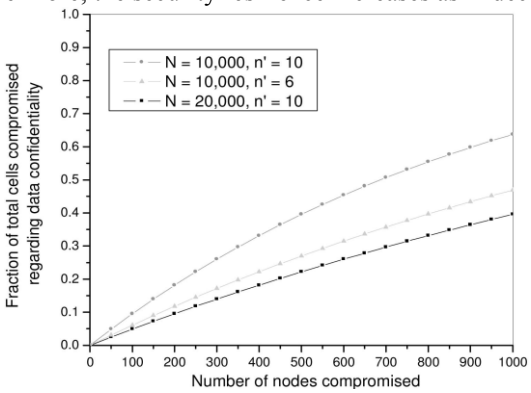


Fig:1

***B. Security Strength Regarding Data Confidentiality***

The data authenticity is affected as the number of compromised nodes increases. Fig 2 shows how the percentage of compromised cells increases very slowly with the increase of a number of compromised nodes. This observation tells us that it is relatively easier for the attacker to insert the bogus reports into the network; however, these bogus reports can be deterministically filtered by the intermediate nodes or the sink.

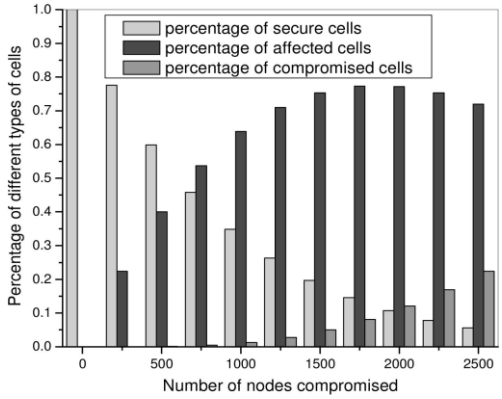


Fig:2

where N = 10000, n′ = 10, and ( e, E) = ( 4, 5 )

***C. Security Strength Regarding Data Availability***

The Fig :3 shows how The Proposed Schema is much more resilient to the report disrupt attacks. In other words, an attacker needs to compromise a lot more nodes to successfully launch report disrupt attacks .

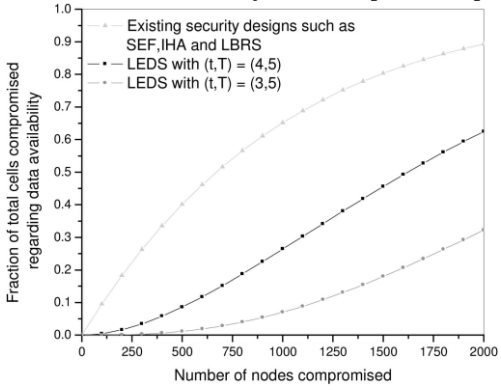


Fig:3

Given N = 10000, n′ = 10, and (e , E) = (4 , 5), to successfully launch a report disrupt attack in 10 percent of
The total cells, around 100 nodes have to be compromised in existing security designs while this number has to be no less than 600 in TDS.

## IX. CONCLUSION

In this paper ,we came up with a Effective Key Management frame work to address the vulnerabilities in existing security designs. In our design each node stores few keys and secret keys are assigned to sensor nodes based on Time Schema. This Time based property successfully limits the impact of compromised nodes only to their vicinity without

 

affecting end-to-end data security. Furthermore, the proposed key management framework assures both node-to-sink and node-to-node authentication along report forwarding routes. We evaluate our design through extensive approach, which demonstrates its high resilience against an increasing number of compromised nodes and effectiveness in computation cost that is, achieving 80 percent.

**REFERENCES**

[1] D. Carman, P. Kruus, and B. Matt, "Constraints and Approaches for Distributed Sensor Network Security," Technical Report 00- 010, NAI Labs, 2000.

[2] A. Wood and J. Stankovic, "Denial of Service in Sensor Networks," Computer, Oct. 2002.

[3] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Ad Hoc Networks, vol. 1, no. 2, 2003.

[4] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar, "SPINS: Security Protocols for Sensor Networks," Proc. MobiCom, July 2001.

[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] 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.

[7] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," Computer, pp. 103-105, Oct. 2003.

[8] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," Proc. IEEE Symp. Research in Security and Privacy, 2003.

[9] 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.

[10] D. Liu and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks," Proc. 10th ACM Conf. Computer and Comm. Security (CCS '03), Oct. 2003.

 