

# A Secure Triple-Key Management Scheme for Wireless Sensor Networks

Tanveer Zia and Albert Zomaya  
 School of Information Technologies  
 University of Sydney, Camperdown NSW 2006  
 Email: {tanzia, zomaya}@it.usyd.edu.au

**Abstract** – Key management is critical to meet the security goals [1] to prevent the Sensor Networks being compromised by an adversary. Due to ad-hoc nature and resource limitations of sensor networks, providing a right key management is challenging. Traditional key management schemes based on trusted third parties like a certification authority are impractical due to unknown topology prior to deployment. In this paper we present a secure triple-key management scheme to provide resilience security against attacks in sensor networks.

**Keywords** – Sensor network security; key management; key calculation

## I. INTRODUCTION

Wireless sensor networks are a promising future of many commercial and military applications. The deployment nature of wireless sensor networks makes them more susceptible to security threats. Due to ad-hoc nature and resource limitations of sensor networks, providing a right key management is challenging. Traditional key management schemes based on trusted third parties like a certification authority (CA) are impractical due to unknown topology prior to deployment. Many solutions have been presented in literature which relies on complex asymmetric and symmetric cryptography which leaves added burden on resource constrained sensor nodes. We are working towards designing a security framework. A naïve idea of our security framework was presented at [2]. Our Wireless Sensor Networks Security Framework (WSNSF) will have a secure hierarchical clustering model, a secure triple-key management scheme, a secure routing mechanism and a mechanism to detect malicious nodes in wireless sensor networks. Our research is motivated by many efforts in key management in wireless sensor networks such as master key based key predistribution scheme, random and extended random key predistribution scheme[4,5], multiple space key predistribution scheme, key management using deployment knowledge[6,7].

In this paper we present our triple-key management scheme. Section II discusses our scheme in detail: calculating base station to node, nodes to cluster leader, cluster leader to cluster leader and then base station keys. In Section III we provide analysis of our secure triple-keys and comparison with TinySec [3] followed by conclusion in Section IV.

## II. SECURE TRIPLE-KEY MANAGEMENT SCHEME

Our secure triple-key management scheme is consisting of three keys: two pre-deployed keys in all nodes and one in-

network generated cluster key for a cluster to address the hierarchical nature of sensor network.

$K_n$  (network key) – Generated by the base station, pre-deployed in each sensor node, and shared by the entire sensor network. Nodes use this key to encrypt the data and pass onto next hop.

$K_s$  (sensor key) – Generated by the base station, pre-deployed in each sensor node, and shared by the entire sensor network. Base station uses this key to decrypt and process the data and cluster leader uses this key to decrypt the data and send to base station.

$K_c$  (cluster key) – Generated by the cluster leader, and shared by the nodes in that particular cluster. Nodes from a cluster use this key to decrypt the data and forward to the cluster leader.

This secure triple-keys management scheme is a much resilient solutions against many of sensor network attacks. We describe below how this scheme works:

### A. Base station to node key calculation

Base station uses  $K_n$  to encrypt and broadcast data. When a sensor node receives the message, it decrypts it by using its  $K_s$ . In figure 1, base station uses  $K_{n.l.m}$  to broadcast the message. This process follows as: Base station encrypts its own ID, a current time stamp TS and its  $K_n$  as a private key. Base station generates a random seed  $S$  and assumes itself at level 0. The packet contains following fields:

$K_n$	MAC	ID	TS	S	message	Level 0
-------	-----	----	----	---	---------	---------

Sensor node decrypts the message received from the base station using  $K_s$ . Here MAC is message authentication code for a message ( $m$ ).

### B. Nodes to Cluster leader key calculation

When node sends a message to cluster leader, it constructs the message as follows:

$$\{\text{ID}_{sn}, K_n, \text{TS}, \text{MAC}, S (\text{message})\}$$

Cluster leader checks the ID from the packet, if the ID in the packet matches the ID it holds, verifies the authentication and integrity of the packet through MAC. Otherwise, packet is dropped by the cluster leader. Node builds the message using the fields below:

$K_n$	MAC	ID	TS	S	message	Level 2
-------	-----	----	----	---	---------	---------

### C. Cluster leader to next hop cluster leader key calculation

Cluster leader aggregates the messages received from its nodes and forwards it to next level cluster leader or if the cluster leader is one hop away from the base station, it directly sends the message to the base station. Receiving cluster leader checks its routing table and constructs the following packet to be sent to next level cluster leader or the base station. Cluster leader adds its own ID  $CL_n$ , its network and cluster key in incoming packet and rebuilds the packet as under:

$$\{ID, K_{CLn}, [ID_{sn}, K_n, TS, MAC, S (Aggr message)]\}$$

$K_n$	$K_c$	MAC	ID	TS	S	Aggr message	Level 1
-------	-------	-----	----	----	---	--------------	---------

Here ID is the ID of receiving cluster leader which wraps the message and sends it to the next hop cluster leader or to the base station if directly connected. Next hop cluster leader receives the packet and checks the ID, if the ID embedded in the packet is same as it holds, it updates the ID for the next hop and broadcast it, or else the packet is discarded. *Aggr message* refers to the message aggregated by the cluster leader.

### D. Cluster leader to base station key calculation

Base station receives the packet from its directly connected cluster leader; it checks the ID of sending cluster leader, verifies the authentication and integrity of the packet through MAC. Cluster leader directly connected with base station adds its own ID along with the packet received from the sending cluster leader. Packet contains the following fields:

$$\{ID_{CL2}[ID_{CL4}, K_n, [ID_{s10}, K_n, TS, MAC, S (Aggr message)]]\}$$

Figure 1 below illustrate the hierarchal structure of our secure triple-key management scheme where we have shown sensor nodes  $S1..S11$ , cluster leaders  $CL1..CL4$  and base station  $BS$  communication using the triple-key management scheme.

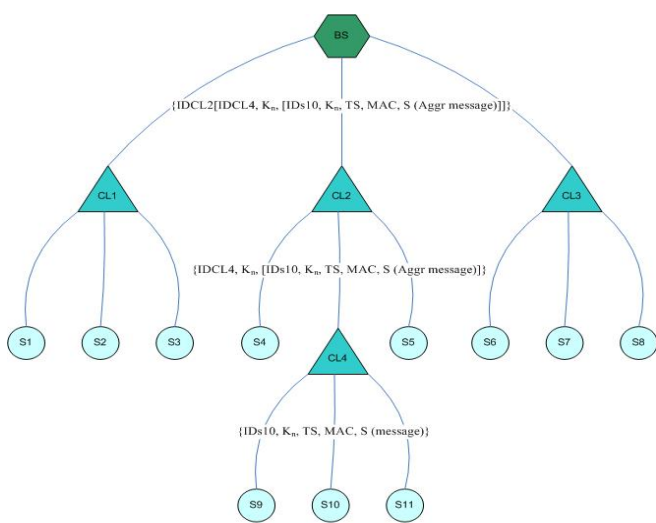


Figure 1. A secure triple-key management

## III. ANALYSIS OF SECURE-TRIPLE KEYS SCHEME

We compare our framework with the TinySec [3]. TinySec is so far the de facto security solution at Berkeley.

Table 1 below lists the TinySec and our secure triple-keys packet overheads. This comparison shows that our triple keys do not have any additional overheads instead it overcomes the weaknesses of TinySec. We have done cryptanalysis of TinySec and found TinySec very confusing e.g., no TinySec, TinySec-Auth and TinySec-AE. Also TinySec assumes a message length of 8 bytes or more, it does not address the smaller messages.

TABLE 1. COMPARISON OF OVERHEADS IN TINYSEC AND TRIPLE-KEYS

	Application Data (b)	Packet Overhead (b)	Total Size (b)	Time to transmit (ms)	Increase over TinyOS stack
CRC	24	39	63	26.2	--
TinySec-Auth	24	40	64	26.6	1.5%
TinySec-AE	24	44	68	28.8	8%
Triple-Keys	24	44	68	28.8	8%

## IV. CONCLUSION AND FUTURE WORK

We have presented a secure triple-key management scheme which provides stronger resilience against susceptible attacks on sensor networks by keeping in mind the resource starved nature of sensor nodes. We plan to implement our secure triple-key management scheme in Berkeley's notes. Eventually this secure triple-key management scheme will become part of our broader security framework for wireless sensor networks.

## REFERENCES

- [1] C.P. Fleegeer, Security in computing, 3<sup>rd</sup> edition, Prentice-Hall Inc. NJ. 2003
- [2] T.A Zia and A.Y. Zomaya, A security framework for wireless sensor networks, *in the proceedings of IEEE Sensor Applications Symposium (SAS06)*, February 7-9 2006, Hoston, Texas, USA
- [3] C. karlof, N. Shastry and D. Wagner, TinySec: A link layer security architecture for wireless sensor networks, *SenSys'04*, November 3-5 2004, Baltimore, Maryland, USA
- [4] L. Eschenauer and V. Gligor, A key-management scheme for distributed sensor networks, *Proceedings of the 9<sup>th</sup> ACM conference on Computer and Communication Security 2002*, Washington DC, USA
- [5] H. Chan, A. Perrig, and D. Song, Random Key Predistribution Schemes for Sensor Networks. *In Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, California USA
- [6] W. Du, J. Deng, Y.S. Han, S. Chen, and P.K. Varshney, A key management scheme for wireless sensor networks using deployment knowledge", *IEEE InfoCom 2004*.
- [7] W. Du, J. Deng, Y.S. Han, P.K. Varshney, A key predistribution scheme for sensor networks using deployment knowledge, *IEEE Transactions on Dependable and Secure Computing*, Vol. 3, Issue 1, Jan-March 2006 pp.62-77.