



Aim

To develop a high level security framework to address threats against Wireless Sensor Networks.

There are two major problems: (1) key management and (2) secure routing in sensor sensor networks.

Security Challenges

The resource constrained nature of WSNs poses unique security challenges. For example:

- Expensive cryptography techniques such as public keys are not practical due to computation and communication constraints. Furthermore, limitations in energy may trigger "resource consumption consumption attacks.
- Sensor nodes are usually deployed in an unattended fashion and are subject to node node capture attacks.
- Sensor net applications often depend on local computation and communication. A determined attacker may attack any node in a network and use use information gathered from compromised compromised nodes to attack non-compromised ones.

Investigated Research Problems

- Key Management
- Secure Routing

Key Management

Problem: How to calculate, deploy and manage secure keys among nodes, cluster cluster leaders and the base station to establish a secure communication?

Challenges: Resource constraints (limited computation, storage, and communication capabilities). Threat of compromised nodes.

Our solution: follows:

Our **secure triple-key management scheme** consists of three keys:

K_n (network key) – A pre-deployed key in in each node, and shared by the network. Nodes use this key to encrypt the the data and pass it to the next hop.

K_s (sensor key) – Pre-deployed in each node, and shared by the entire network. BS BS uses this key to decrypt and process the the data and CL uses this key to decrypt the the data and send to BS.

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

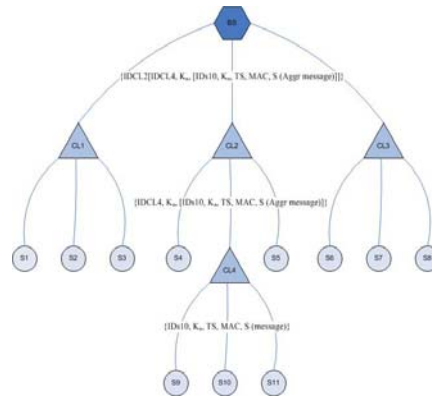


Figure 1: Secure triple-key management scheme. Key Key calculation from node to CL (Cluster Leader), CL CL to CL and CL to the Base Station

Table 1: Analysis of triple key management scheme

	Data packets (b)	Packet Overhead (b)	Total Size (b)	Time xmit (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%

Secure Routing

Problem: How to detect bogus and replayed routing information WSNs?

Challenges: Spoofed, replayed routing information, Sybil and HELLO flood attacks.

Our solution: follows:

Our Secure Routing algorithms

Base station algorithm:

Base station algorithm is responsible of following tasks:

- Broadcasting of K_s and K_n by the base base station
- Decryption and authentication of data by data by the base station

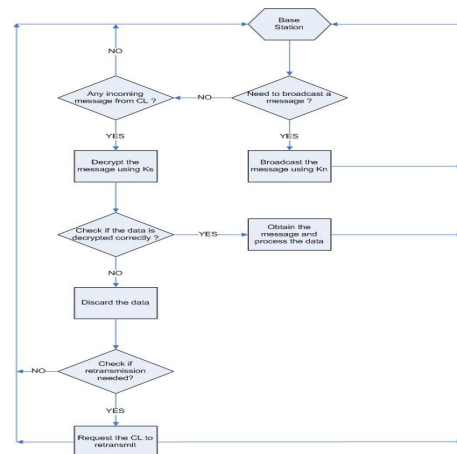


Figure 2: BS to CL and node communication

Node algorithm:

Node algorithm performs the following functions:

- Sensor nodes use the K_n to encrypt and and transmit the data
- Transmission of encrypted data from nodes to cluster leader
- Appending ID# to data and then forwarding it to higher level of cluster leaders
- Cluster leader uses K_c to decrypt and and then uses its K_n to encrypt and send the data to next level of cluster leaders, eventually reaching the base station.

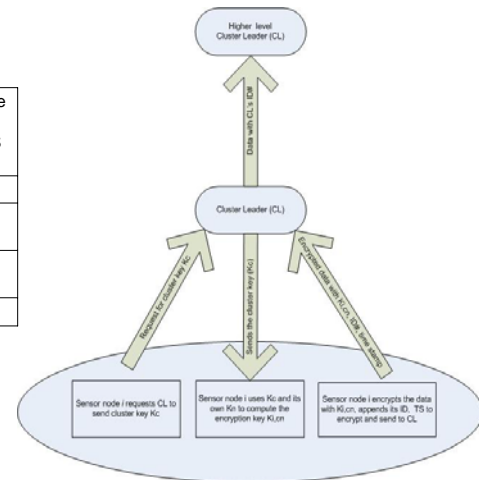


Figure 3: Sensor node i to Cluster Leader and base station communication

Summary

Triple key management scheme and routing routing algorithms presented in this framework framework takes into consideration the nodes nodes and cluster leaders which are not participating in sending and aggregating the the data. These nodes forward the data packets without applying any further cryptographic operation, thus further saving the saving the processing power and memory. We are investigating other security issues such such as malicious node detection and secure secure localization and plan to add the the solutions in our framework.

References

Zia, T.A., and Zomaya, A.Y., "A Secure Triple-Key Management Scheme for Wireless Sensor Networks", In In the proceedings of the IEEE InfoCom 2006 Students Workshop, April 23-24, 2006, Barcelona, Spain

Zia, T.A, and Zomaya, A. Y., "A Security Framework for Wireless Sensor Networks", In the proceedings of the IEEE IEEE Sensor Applications Symposium (SAS06), February 7-9, 2006 , Houston, Texas.