An Efficient Key Management Scheme for Wireless Network

Yogendra Kumar Jain, Vismay Jain

Abstract-Sensor networks have great potential to be employed in mission critical situations like battlefields but also in more everyday security and commercial applications such as building and traffic surveillance, habitat monitoring and smart homes etc. However, wireless sensor networks pose unique security challenges. While the deployment of sensor nodes in an unattended environment makes the networks vulnerable to a variety of potential attacks, the inherent power and memory limitations of sensor nodes makes conventional security solutions unfeasible. Key Management is a major challenge to achieve security in wireless sensor networks. In most of the schemes presented for key management in wireless sensor networks, it is assumed that the sensor nodes have the same capability. This research presents a security framework WSNSF (Wireless Sensor Networks Security Framework) to provide a comprehensive security solution against the known attacks in sensor networks. The proposed framework consists of four interacting components: a secure triple-key (STKS) scheme, secure routing algorithms (SRAs), a secure localization technique (SLT) and a malicious node detection mechanism. Singly, each of these components can achieve certain level of security. However, when deployed as a framework, a high degree of security is achievable. WSNSF takes into consideration the communication and computation limitations of sensor networks. While there is always a tradeoff between security and performance, experimental results prove that the proposed framework can achieve high degree of security, transmission overheads and perfect resilience against node capture.

Keywords- Wireless Sensor Networks, Secure triple key, Routing algorithms, Localization technique.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) have recently attracted much attention because of their wide range of application, such as military, environmental monitoring, and heath care industry. Unlike wired and Mobile Ad hoc Networks, wireless sensor networks are infrastructure-less and can operate in any environment as compared to the traditional networks. Wireless sensor networks mainly consist of large number of tiny and simple nodes that are randomly deployed in operating areas unattended. In hierarchical WSNs, sensor nodes are clustered and a gateway or cluster head is allocated for each cluster. Gateway nodes are more powerful in computational capability, memory storage, life time, and communication range as compared to other nodes [1]. In this paper, we propose a framework for key management in cluster based WSNs using a hybrid technique of public key and symmetric key cryptography. A symmetric key is assigned dynamically to sensor nodes to establish a secure link with their neighbors. A public key is pre-loaded to the sensor nodes and gateways for communicating with each other. Because gateway nodes are powerful, using Elliptic Curve Cryptography (ECC) as a lightweight public key cryptography would not provide overhead in the network. Advancements in Micro Electro Mechanical Systems (MEMS) and wireless networks have made possible the advent of tiny sensor nodes sometimes referred as “motes”. These are mini, low-cost devices with limited coverage having low power, smaller memory sizes and low bandwidth. Wireless sensor networks consist of a large number of such sensor nodes and are able to collect and disseminate data in areas where ordinary networks are unsuitable for environmental and/or strategic reasons. As such, they have a promising future in many applications, such as smart houses, smart farms, smart parking, smart hospitals, habitat monitoring, building and structure monitoring, distributed robotics, industry and manufacturing, national security etc. The sensors’ low cost has made wireless sensor networks more viable and have contributed to their increasing popularity as potential low-cost solutions to a variety of real life challenges. While all networks are subject to common threats, remote wireless sensor networks are additionally vulnerable to security breaches because they are physically more accessible to possible adversaries. The memory and energy limitations of sensor nodes are a major obstacle to implementing traditional security solutions. The fact that wireless sensor networks utilise unreliable communication media and are left unattended once deployed makes the provision of adequate security countermeasures even more difficult [2], [3], [7] and [13].

2. BACKGROUND

Wireless sensor networks have unique constraints as compared to traditional networks making the implementation of existing security measures not practicable. In broader terms, these constraints are the result of limitations regarding the sensor nodes' memory, energy, transmission and processing power as well as due to the ad-hoc and wireless channel. These constraints, which make the design of security procedures more complicated, have been categorised into node constraints and network constraints. The security solutions require high computation, memory, storage and energy resources which creates an additional challenge when working with tiny sensor nodes. Typical sensor nodes are tiny devices which come with very limited memory and storage capacity. Berkeley's MICA2 possess 4-8 MHz, 4KB of RAM, 128KB flash and ideally 916 MHz of radio frequency .This means any security solution designed for sensor networks should be smaller in code. Energy is another important factor to consider when designing security measures for sensor nodes. Given the sensor network topology which makes accessing them after deployment impracticable, it is very important to limit the energy consumption and thereby extend the battery life. However, adding security measures to sensor networks necessarily has a significant impact on its energy consumption, for example, to perform the encryption and decryption functions, to store, manage and send the encryption keys etc. Sensor networks inherit all the constraints of mobile ad hoc networks such as unreliable network communication, collision related problems and their lack of physical infrastructure. Wireless communication is inherently unreliable and can cause packets to be damaged or dropped. This unreliability in communication poses additional threats to the nodes if dropped packets are taken over by adversaries. The networks utilise a dense arrangement of nodes potentially deploying hundreds of thousands of nodes in a sensitive application. This raises the likelihood of collision and latency in packets. However, unlike in traditional networks, the energy limitations of sensor nodes makes it impracticable to resend packets in case of collision [2], [12] and [13].
Setting security goals for sensor networks will depend on knowing what it is that needs protecting. Sensor networks share some of the features of mobile ad hoc networks but also pose the unique challenges discussed in the previous. Therefore the security goals encompass both those of the traditional networks and goals suited to the unique constraints of sensor networks. The four security goals for sensor networks are determined as Confidentiality, Integrity, Authentication and Availability (CIAA) [4], [9] and [10].

Recently, the probabilistic key pre-distribution scheme where each sensor node receives a random subset of keys from a large key pool before deployment. To agree on a key for communication, two nodes find one common key within their subsets and use that as their shared key. To extend this idea with three key pre-distribution schemes: a q-composite scheme, multi-path reinforcement, and a random-pair-wise key scheme [6], [14] and [15].

Probabilistic model using random key assignment and two protocols 'direct' and 'cooperative' to establish pair-wise communication between sensors by assigning a small set of random keys to each sensor. This idea is later converged into the pseudo random generation of keys which is more energy efficient compared to previous key management schemes. General framework for establishing pair-wise keys between sensors on the basis of a polynomial-based key pre-distribution protocol . They later present two instantiations of the general framework: a random subset assignment key pre-distribution scheme, and a hypercube-based key pre-distribution scheme. Finally, they also propose a technique to reduce the computation at the sensors so that their scheme could be implemented efficiently [3], [5] and [11].

In previous, a pair-wise key pre-distribution is an effort to improve the resilience of the network by lowering the initial payoff of smaller scale network attacks and pushing the adversary towards a larger scaled attack to compromise the network.
In later work present a key scheme based on deployment knowledge. This key management scheme takes advantage of the deployment knowledge where the sensor's position is known prior to deployment. Because of the randomness of deployment, it is not feasible to know the exact location of neighbours, but it is realistic to know the set of likely neighbours. This issue is addressed using the random key pre-distribution [2], [8] and [16].
The secure localization technique based on the use of directional antennas. Referring to

applications where the sensor nodes need to be disguised, having directional antennas is not feasible, use explicit RF distance bounding in order to obtain a verifiable location in the presence of attackers. This scheme utilises the known position of certain nodes as "landmarks". However, since these landmarks are placed across the network in an organized manner, this could pose some difficulty in applications such as on a battlefield where the nodes are deployed by being dropped from aircrafts. In such cases, determining the landmarks' positions may not be practical then [1].

3. PROPOSED TECHNIQUE

3.1 Secure Triple Key Scheme (STKS):

Based on the argument that no single keying method provides adequately secure communication in sensor networks, a secure triple-key (STKS) scheme is proposed consisting of three keys: two pre-deployed keys in all nodes and one in-network generated cluster key which addresses the hierarchical nature of sensor network. The network key K_n is generated by the base station, pre-deployed in each sensor node, and shared by the entire sensor network. The nodes use this key to *encrypt* the data before passing it on to the next hop. The sensor key K_s is generated by the base station, pre-deployed in each sensor node, and shared by the entire sensor network. The base station uses this key to *decrypt* and process the data, and the cluster leader uses this key to *decrypt* the data and send it to the base station. The cluster key K_c is 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. Nodes will only use this key when they are serving as a cluster leader, otherwise they do not need to decrypt messages received from other nodes thus saving the energy and processing power. This triple key serves the purpose of confidentiality and authentication, and the following section describes how the scheme works.

3.2 Terms and Notations Used:

The following terms and notations are used in the secure triple key scheme (STKS).

ID# → The unique ID of the sensor node.
TS → An encrypted time stamp for beacon authentication.
Aggr Message → Message aggregated by a cluster leader.
CL→ Cluster leader – a node randomly elected as a leader for a given group of sensors through an election process.
BS→ Base station, a node assumed to be very powerful with extraordinary computation resources.
MAC_k (M) → Message authentication code for message *m*, generated using key *k*.
K_n → Network key (Kn) – generated by the base station, broadcast and shared throughout the network.
K_s → Sensor key (Ks) – generated by the base station, based on a seed and sensor ID, pre-deployed in each sensor node and shared by the sensor nodes and base station.
K_c → Cluster key (Kc) – generated by the cluster leader and shared by the nodes in that particular cluster.

3.3 Base Station to Node Key calculation:

The base station uses its network key K_n to encrypt and broadcast data. When a sensor node receives this message, it decrypts it using its sensor key K_s. This proceeds as follows: The base station encrypts its own ID, a time stamp *TS* and its network key K_n. The packet contains following fields:

K_n	MAC	ID	TS	Message

The sensor node decrypts the message received from the base station using its sensor key K_s whereby the MAC is the authentication code for a message (*m*).

3.4 Proposed Secure Routing Algorithms (SRAs):

In the proposed secure routing mechanism all the nodes have a unique ID# to uniquely identify the sensor nodes. Once the network is deployed, the base station builds a table containing ID#s of all the nodes in the network. After a self-organizing process the base station knows the topology of the network. The nodes use the proposed secure triple-key scheme (STKS) to encrypt and authenticate the collected data, and then forward it to the cluster leader which aggregates and sends the data to the base station. The energy efficient secure data transmission algorithms were adapted and modified with the secure triple-key scheme (STKS) to make transmission resilient against attacks. The two algorithms used to securely transfer the data from the nodes to the base station and vice versa are the sensor node algorithm and the base station algorithm. These are presented below.

3.4 Node algorithm performs the following functions:

→Sensor node uses the *Kn* to encrypt 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. (In hierarchical topology, cluster leaders closer to the base station is known as a high level cluster leader)

→Cluster leader uses *Kc* to decrypt and then uses its *Kn* to encrypt and send the data to next level of cluster leaders, eventually reaching the base station

3.5 Base station algorithm is responsible for following tasks:

→Broadcasting of *Ks* and *Kn* by the base station

→Decryption and authentication of data by the base station

Node Algorithm:
The node algorithm performs the following functions:

Step 1: If Sensor Node *i* wants to send data to its cluster leader, it goes to Step 2; if not, it exits the algorithm.

Step 2: Sensor Node *i* requests the cluster leader to send *Kc*.

Step 3: Upon receipt, Sensor Node *i* uses *Kc* and its own *Kn* to compute the encryption key.

Step 4: Sensor Node *i* encrypts the data with *Kn*, appends its ID# and the *TS* to the encrypted data and then sends this to the cluster leader.

Step 5: The cluster leader receives the data, uses *Ks* to decrypt it and aggregates the data. It then appends its own ID#, adds the *TS* and encrypts the data using *Kc*, whereupon it sends it to the higher-level cluster leader or to the base station if directly connected. Thereafter it begins again at Step 1.

Figure1 below demonstrates how this algorithm proceeds and illustrates the communication between Sensor Node *i* and the cluster leader.

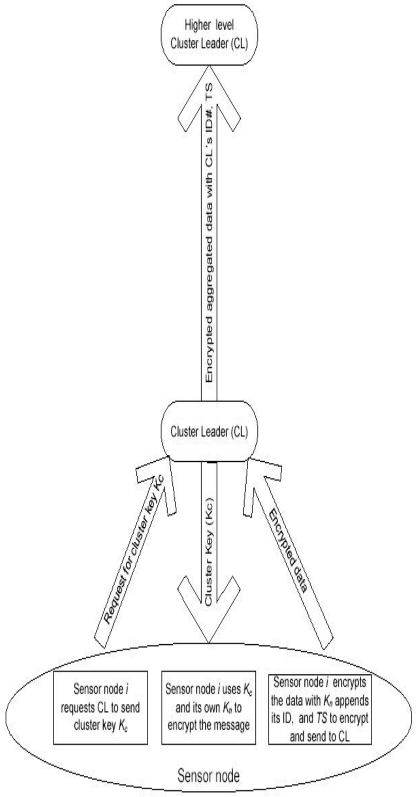
Higher level Cluster Leader (CL)
Encrypted aggregated data with CL's ID#, TS
Cluster Leader (CL)
Request for cluster key Kc
Cluster Key (Kc)
Encrypted data
Sensor node *i* requests CL to send cluster key K_c
Sensor node *i* uses K_c and its own K_n to encrypt the message
Sensor node *i* encrypts the data with K_n appends its ID, and *TS* to encrypt and send to CL
Sensor node

Figure1 Sensor Node *i* to cluster leader and base station communication.

Base Station Algorithm:

According to the suggested algorithm the base station performs these steps:

Step 1: Check if there is any need to broadcast a message. If so, broadcast the message encrypting it with *Kn*.
Step 2: If there is no need to broadcast a message then check if there are any incoming messages from the cluster leaders. If there is no data being sent to the base station return to step 1.

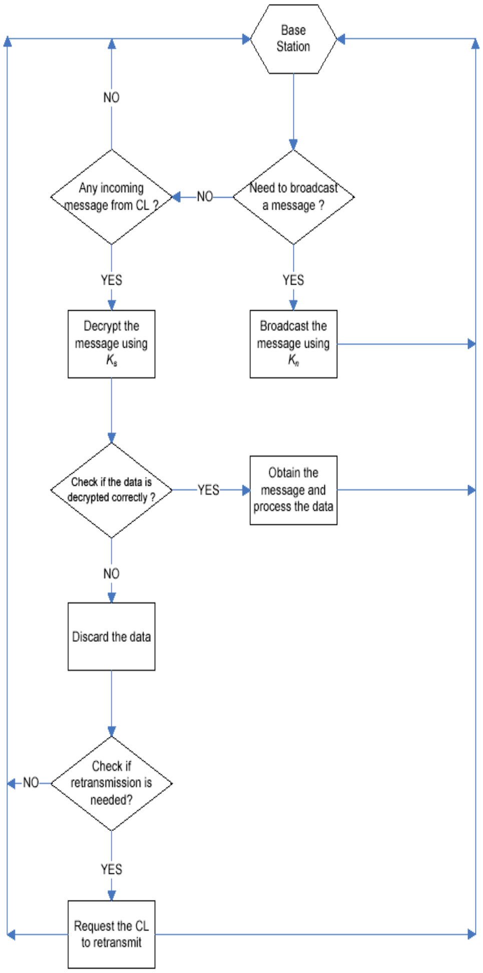
Base Station
Need to broadcast a message ?
NO
Any incoming message from CL ?
NO
YES
YES
Broadcast the message using K_n
Decrypt the message using K_s
Check if the data is decrypted correctly ?
YES
Obtain the message and process the data
NO
Discard the data
Check if retransmission is needed?
NO
YES
Request the CL to retransmit

Figure 2 Base stations to cluster leader and sensor node communication.

Step 3: If there is any data coming in to the base station then decrypt it using *Ks*, the ID# of the node and the TS within the data.

Step 4: Check if the decryption key *Ks* has decrypted the data perfectly by checking the credibility of the TS and the ID#. If the decrypted data is not perfect, discard the data and go to Step 6.

Step 5: Process the decrypted data and obtain the message sent by the cluster leaders and sensor nodes.

Step 6: Decide whether to request all sensor nodes for retransmission of data. If deemed not necessary, return to Step 1.

Step 7: If a request is necessary, send one to the sensor nodes asking them to retransmit the data. Once this session is finished, return to Step 1.

This routing technique using the secure triple-key management scheme provides a strong resilience against the spoofed routing information attacks, selective forwarding, sinkhole attacks, Sybil attacks, wormholes, and HELLO flood attacks.
The Figure 2 illustrates the base station to node algorithm:

4. RESULTS

The level of this scheme's security depends entirely on the application. The percentage of neighbours being awake all the time could be providing complete security. Instead, in order to be more energy efficient, the topology works by letting each node go to sleep when it is not sending or receiving a packet. As seen from the experimental results shown in Figure below, the time required to detect a malicious node decreases when the number of nodes in the network is increased. This is because in dense network, the probability of node detection is higher and faster because there are more neighbours monitoring the nodes. The results in Figure are an average of 10 runs.

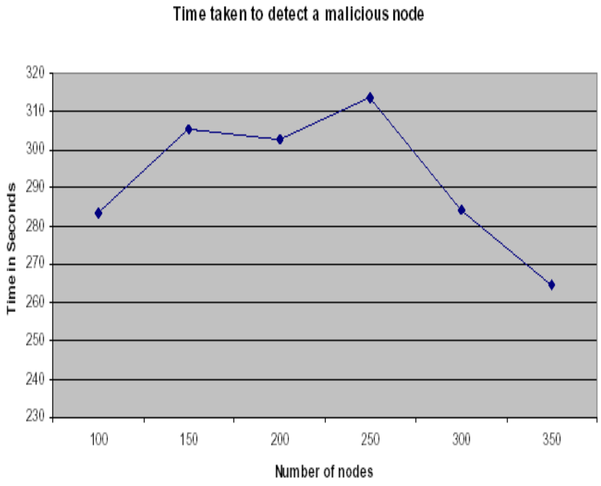

Figure 3 Time taken to detect a malicious node.

5. CONCLUSION AND FUTURE WORK

Traditional security measures require heavy communication and computational resources which are beyond the resource starved sensor nodes. In this research, it has been argued that cryptographically complex security solutions for sensor networks are not viable for many reasons: firstly, the energy, memory and transmission range limitations; secondly, the wireless channel limitations; thirdly, the deployment nature of sensor nodes being left unattended after deployment; and fourthly, the need to keep costs low to enable dense deployment. Instead, sensor networks need a balanced and comprehensive solution, which is efficient, effective and has low security overheads. Bearing these factors in mind, a novel security framework for wireless sensor networks has been proposed. We are heading towards a future of miniature station and wireless connectivity and sensor networks have the ability to deliver both at very low cost. For future research we propose extending this security framework to include trust establishment and trust management in sensor networks. Besides this we have an interest in exploring and solving security issues in multimedia and biometric security, cyber security and information assurance, protection against identity theft, and forensic computing.

6. REFERENCES

[1] Reza Azarderakhsh, Arash Reyhani-Masoleh, and Zine-Eddine Abid, “A Key Management Scheme for Cluster BasedWireless Sensor Networks “,2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing.

[2] Asif Habib, “Sensor Network Security Issues at Network Layer” 2nd International Conference on Advances in Space Technologies, IEEE 2008.

[3] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou, “Sensor Network Security: A Survey” ,IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 11, NO. 2, SECOND QUARTER 2009.

[4] Anderson, R., Chan, H. and Perrig, A. (2004) Key infection: smart trust for smart dust. In Proceedings of the 12th IEEE International Conference on Network Protocols, Oct 5-8, 2004,

[5] Anjum, F., Pandey, S. and Agrawal, P. (2005) Secure localization in sensor networks using transmission range variation. In Proceedings of IEEE MASS 2005 Workshop, November 7-11, 2005.

[6]Axelsson, S. (2000) Intrusion detection systems: a survey and taxonomy. Research Report. 15 March 2000. Göteborg, Sweden, Department of Computer Engineering, Chalmers University of Technology. Available at http://www.mnlab.cs.depaul.edu/seminar/spr2003/IDSSurvey.pdf [Accessed 16 June 2007]

[7]Cam, H., Ozdemir, S., Muthuavinashiappan, D. and Nair, P. (2003) Energy efficient security protocol for wireless sensor networks. In Proceedings of 58th IEEE Vehicular Technology Conference, Oct. 6-9, 2003,

[8]Chan, H., Perrig, A. and Song, D. (2003) Random key redistribution schemes for sensor networks. In Proceedings of the IEEE Symposium on Security and Privacy, 11-14 May 2003.

[9]Choi, S.H., Kim, B.K., Park, J., Kang, C.H. and Eom, D.S. (2004) An implementation of wireless sensor networks. IEEE Transactions on Consumer Electronics.

[10] Chong, C.Y. and Kumar, S.P. (2003) Sensor networks: evolution, opportunities and challenges. IEEE Transactions on Consumer Electronics.

[11] Du, W., Deng, J., Han, Y., Chen, S.S. and Varshney, P.K. (2004) A key management scheme for wireless sensor networks using deployment knowledge. In Proceedings of the IEEE InfoCom, March 7-11, 2004.

[12] Jianmin Zhang, Qingmin Cui and Xiande Liu, “An Efficient Key Management Scheme for Wireless Sensor Networks in Hostile Environments”, IEEE 2009 International Conference on Multimedia Information Networking and Security.

[13] C.Gnana Kousalya and Dr.J. Raja, “An Energy Efficient Traffic-Based Key Management Scheme for Wireless Sensor Networks ” IEEE 2009 International Conference on Networking and Digital Society.

[14] Xing Zhang, Jingsha He and Qian Wei, “An Energy-Efficient Dynamic Key Management Scheme in Wireless Sensor Networks”, IEEE 2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks.

[15] Yong Ho Kim, Hwaseong Lee, and Dong Hoon Lee, “A secure and efficient key management scheme for wireless sensor networks”, This research was supported by the MIC(Ministry of Information and Communication), Korea, (IITA-2006-(C1090-0603-0025)).

[16] Guorui Li, Ying Wang and Jingsha He, “Efficient Group Key Management Scheme in Wireless Sensor Networks”, IEEE 2010 Third International Symposium on Intelligent Information Technology and Security Informatics.

7. AUTHORS PROFILE

Dr. Yogendra Kumar Jain presently working as head of the department, Computer Science & Engineering at Samrat Ashok Technological Institute Vidisha M.P India. The degree of B.E. (Hons) secured in E&I from SATI Vidisha in 1991, M.E. (Hons) in Digital Tech. & Instrumentation from SGSITS, DAVV Indore (M.P), India in 1999. The Ph. D. degree has been awarded from Rajiv Gandhi Technical University, Bhopal (M.P.) India in 2010. Research Interest includes Image Processing, Image compression, Network Security, Watermarking, Data Mining. Published more than 40 Research papers in various Journals/Conferences, which include 10 research papers in International Journals. **Tel**:+91-7592-250408, **E-mail**: ykjain_p@yahoo.co.in.

Mr. Vismay Jain presently pursuing M.Tech of the department, Computer Science & Engineering at Samrat Ashok Technological Institute, Vidisha, M.P., India. The degree of B.E. secured in Information Technology from S.A.T.I., in 2008. Research Interest includes Network Security, Data Mining, Artificial Intelligence. **Mobile:** +91-9424445773. **E-mail:** jain.vismay@gmail.com