A Novel Secure Keying Technique for the Wireless Sensor Networks

Kalpana Sharma, M. K. Ghose, Jr, and V. K. Singh

***Abstract*—Strong cryptographic schemes are used for securing the Wireless Sensor Networks (WSNs). Even if a strong cipher is used for encryption/ decryption of messages in any form of WSN communication, if the key is compromised and it no longer remains secret, the security of the underlying network is compromised. Therefore key management schemes play a very vital role in the maintenance of security of any system. This paper deals with a secure key management scheme for the WSN which does not rely on a single key. Rather this scheme uses a combination of all key types like *'in-network generated keys'*, *'broadcasted keys'* and *'pre-deployed keys'* to come up with a robust keying mechanism for the WSN.**

***Index Terms*— Cipher, key management, security, WSN.**

I. Introduction

Wireless Sensor Networks (WSN) is a special kind of networks which consist of a hundreds and thousands of tiny nodes, deployed in an area of interest to accomplish a particular mission. There are basically four types of communication traffic in a WSN environment. These are one to one, many to one, many to many and one to many. In order to secure the whole WSN, all communication types needs to be secured. Using secure keying techniques the messages are securely routed by the nodes and the Cluster Heads (CH) to the Base Station (BS).

Each keying techniques have their own strengths and weaknesses as listed in Table I. Thus a good keying mechanism should consist of a combination of variety of keying techniques like 'in-network generated keys', 'pre-deployed keys' and 'broadcast keys' [1]. The design of the secure keying module presented in this paper is motivated by the fact that different types of messages exchanged between sensor nodes have different security requirements, and that a single keying mechanism is not suitable for meeting these different security requirements.

The rest of the paper has been organized as follows: section 2 deals with the background on the various key management schemes followed by section 3 which deals with the details on the secure keying technique presented in this paper. This section covers key usage, key maintenance and key refreshment. Section 4 deals with the results and discussion followed by conclusion in section 5.

II. Literature Survey

John Paul Walters et al. have discussed various key establishments and associated protocol in [2]. Perrig et al. [3] introduce 'SPINS' which comprises of Sensor Network Encryption Protocol (SNEP) and TESLA. The function of SNEP is to provide confidentiality, authentication, integrity and freshness and TESLA is to provide authentication to data broadcasts. SPINS presents an architecture where the BS accesses nodes using source routing. Four different keying mechanisms are provided by LEAP [4]. The scheme for pre-key distribution based on the prior deployment knowledge of the sensor nodes is discussed in [5]. New schemes for key management for confidential communication between node and its cluster head in hierarchical sensor networks is discussed in [1].These schemes exhibit better performance with some additional storage. Zia et al. [6] have discussed secure triple-key management scheme. In [7] the authors have presented a security framework discussing the cluster formation and leader election process, secure key management scheme, secure routing and their algorithms. Mann et al. describes a novel re-keying function protocol for the WSN network security in [8] covering keying aspects like key establishment, deployment and key refreshment. Yue et al. [9] and Boyle et al. [10] have given an overview on key establishment and agreement protocols in their papers. Key agreement protocol in [11] by Bresson et al. is an authenticated group key agreement protocol.

TABLE I: Comparison of Keys

Key Type	Strengths /Weaknesses
In-Network generated keys	Strengths: 1.Can achieve a high- level security for node-node communication 2.Less communication required 3. If node compromised, only the group key would be available to the attacker but not the entire network's Weaknesses: Increases both computation and communication overhead.
Pre-deployed keys	Strengths: 1.Easy to imprint 2.Doesnot incur communication cost Weaknesses: 1. Vulnerable to node capture attack as the key may be exposed. 2. Leads to a non-scalable network
Broadcasted keys	Strength: 1. Such keys are difficult to break as it is generated by a powerful BS. Main Weakness: Increases communication overhead

Manuscript received March 7, 2012; revised May 22, 2012.

The authors are with the Computer Science and Engineering Department, Sikkim Manipal Institute of Technology, Sikkim, India (e-mail: kalpanaiitkgp@yahoo.com, mkghose2000@yahoo.com, vikashsmit2009@gmail.com)

III. Proposed Key Management Scheme

A single keying technique is not appropriate to secure all the communication types of the WSN. The key management module of this paper does not rely on a single key type but makes use of a combination of keying techniques like '*in-network generated keys*', '*pre-deployed keys*' and '*broadcast keys*'. The various keys used in the proposed scheme are presented in section A.

A. Key Types for Keying Scheme

Once the 'neighbor discovery'phase is over, the BS initiates the key distribution process. In general pair-wise key distribution scheme is set up between the neighbors.

The following keys are used in the proposed protocol:

1) Buddy key (Kb) is calculated by all the nodes after neighbor finding phase is over.
2) My-Own-Key (Ko): All the nodes are preloaded with its id and is used for Ko calculation.
3) Network key (Kn): When a node wants to join the network it sends a request to the BS for acquiring network key kn. Only the node which is authentic acquires Kn.
4) Cluster Key (Kc) is calculated by the CHs.
5) Broadcast Key (Kbro) is issued by the BS after authentication as CHs.

The keys used in this proposed keying scheme are listed in the Table II.

TABLE II: Keys used

Key type	Key Calculation
Ko	f(node-id,sector-id,remaining energy level)
Kb	Idsender + f (Idreceiver ,track-id).
Kn	Calculated by the BS
Kbro	Calculated by the BS
Kc	f(node id, sector-id, track-id).

B. Phases of the Keying Scheme

In order to develop a secure keying scheme, key management scheme presented in this paper is divided into various phases as shown in Fig. 1.

Phase1: Key Pre-distribution

Phase2: Topology formation & Neighbor finding

Phase 3: Calculation of the first basic key ko.

Phase 4: Authentication of the nodes to acquire network wide key kn.

Phase 5: In-Network key calculation and/or Broadcasted key acquisition.

Phase 6: Periodic key-refreshment and maintenance

Fig. 1. Phases of the keying scheme.

Phase 1: Key pre-distribution: All the nodes have node-id imprinted on them before deployment. Node-id is used for Ko calculation.

Phase 2: Topology formation and Neighbor finding phase is described in detail in [12]. To summarize, a hierarchical clustered topology is adapted. The whole network is divided in tracks and sectors, details of which are available in [13], in order to restrict the communication within a sector or a group only. After this phase, the selection of Cluster Heads (CHs) per sector is done. Two CHs viz. the Data Cluster Head (DCH) and Routing Cluster Heads (RCH) per sector is selected by the BS, the details pertaining to DCH/RCH is available in [12].

Phase 3: Calculation of Ko as listed in table 2.

Phase 4: Node authentication by the BS as shown in Fig. 2.

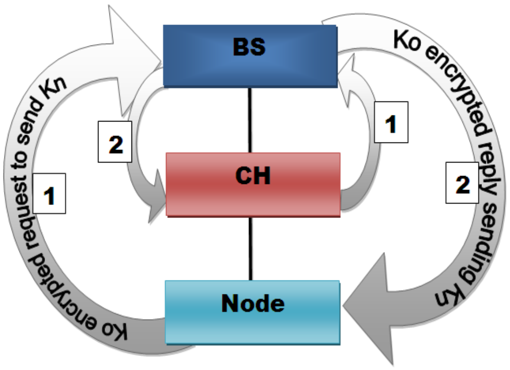
BS
CH
Node
Ko encrypted request to send Kn
Ko encrypted reply sending Kn
1
2
1
2

Fig. 2. Node authentication.

Phase 5: It consists of acquition of in-network keys and broadcast keys. In-network key calculation consists of (a) Establishment of pair wise key (Kb) between neighbors and (b) Establishment of Kc between the DCH and RCH pair as shown in Fig. 3.

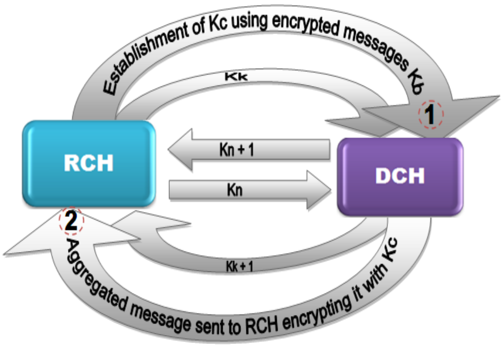
Establishment of Kc using encrypted messages Kb
Kk
1
RCH
Kn + 1
Kn
DCH
2
Kk + 1
Aggregated message sent to RCH encrypting it with Kc

Fig. 3. Establishment of Kc.

Snapshots of the various communications are provided through Fig. 4 & 5.

Broadcasted key acquition: This basically consists of (a) Communication between the BS and all the nodes of the network regarding the role of CH and (b) Request to acquire Kbro by the CHs.

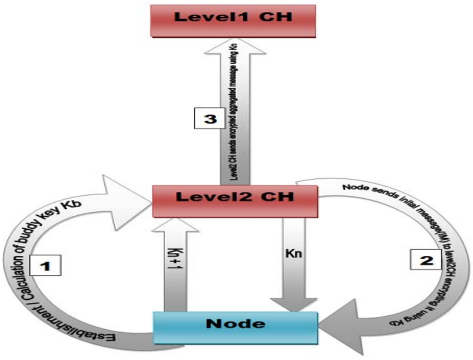
Level1 CH
3
Level2 CH sends encrypted aggregated message using Kn
Level2 CH
Establishment / Calculation of buddy key Kb
1
Kn + 1
Kn
Node sends initial message(IM) to level2CH encrypting it using Kb
2
Node

Fig. 4. Network key request to BS.

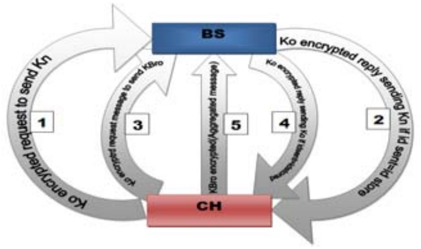
BS
Ko encrypted request to send Kn
1
Ko encrypted request message to send Kbro
3
Kbro encrypted(Aggregated message)
5
4
Ko encrypted reply sending Kn if Id sent=id store
2
CH

Fig. 5. Request for kbro to BS.

Phase 6: Key refreshment/ maintenance: As the role of CH is rotational, Kbro which is calculated by RCH, is refreshed each time the CH changes. Also Kn is refreshed by the BS at regular interval of time. The key refreshment ensures that the nodes belonging to the network is well authenticated from time to time. Also each node in the network maintains the table of all the keys mentioned in Table II.

C. *Key Usage*

All the nodes calculate their own key Ko. Also all the authentic nodes possesses Kn to take part in the communication as Kn is used for encrypting/ decrypting all the messages broadcasted by the BS from time to time. Let the initial message to be sent to the DCH by the ordinary node be IM. This first message format would refer to “(1)”.

$$\text{Message(M)} = \{ \text{Kb, TS,MAC, IM} \} \tag{1}$$

Here TS is the timestamp used to avoid replaying of the messages, MAC is used for authenticating the message. This first message is encrypted using Kb because RCH/DCH is nothing but a buddy to the node in the same sector.

DCH and RCH communicate with each other using cluster key Kc. DCH and RCH compute their cluster-key which is simply a function of their own id, sector-id and track-id. Here sector id may be dropped but for generalization sector id is also considered though all the DCH and RCH should belong to the same sector. But to address the situations where RCH may not be directly communicating with the BS in hierarchical clustering topology of the network, a DCH may have to communicate with DCH or RCH of the cluster of the next higher level. So sector id is retained. DCH, RCH communication is encrypted using cluster key. Since DCH is responsible for data aggregation DCH would send the aggregated message to RCH encrypting it using the Kc and the message format would refer to “(2)”.

$$\text{DCH Message (DM)} \tag{2}$$

$$= \{ \text{Kc},\{ \text{Kb, TS,MAC, aggregated (M)} \} \}$$

The number of nodes in a particular sector varies .If the number of nodes is less than that of the minimum threshold set for the network, RCH acts as both DCH and RCH to save energy.

Now for CH to BS communication, apart from Kc, another key called Kbro is needed. To get hold of Kbro, DCH/RCH sends the request message to BS encrypting it using its own-key K0. BS knows which node has dual function as RCH, DCH and which all have separate DCH, RCH. Accordingly it sends a Kbro to the requesting CH encrypting them with my-own-key of the requesting nodes. So once DCH, RCH acquire the Kbro, communication to RCH to BS takes place encrypting the message by Kbro and the message format looks like this:

RCH Message(RM) = { Kbro,{ Kc,{ Kb, TS,MAC, (DM)}}}

Fig. 6 shows the key exchanges in the proposed keying scheme.

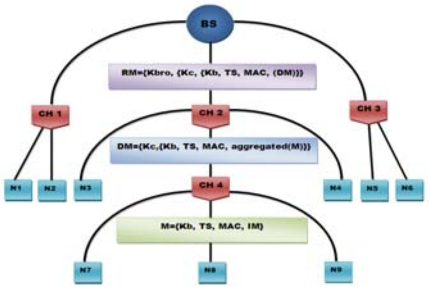
BS
RM={Kbro, {Kc, {Kb, TS, MAC, (DM)}}
CH 1
CH 2
CH 3
DM={Kc,{Kb, TS, MAC, aggregated(M)}}
N1
N2
N3
CH 4
N4
N5
N6
M={Kb, TS, MAC, IM}
N7
N8
N9

Fig. 6. Key setup.

IV. Performance Comparison

The performance of the proposed keying scheme is done in terms of packet size, computational overhead and storage overhead. The format of the proposed packet is shown in Fig. 7.

Keys+ ids	MAC	TS	L	Data
9	4	1	1	29

Fig. 7. Proposed packet format

All the in-network generated keys are the function of node-id, sector-id, track-id, therefore, at most (5+1+1+1+1) bytes i.e. 9 bytes are required for key and id storage. MAC is used for message authentication and integrity. All the values are in bytes. The data packet is not more than 44 bytes long which can be transmitted easily in sensor nodes available in the market today.

A. *Computation Overhead*

The comparison of packet size overhead for TinySec, TripleKey and the proposed scheme is shown in Table III. The values pertaining to TinySec is obtained from [14] whereas TripleKey values are obtained from [6]-[7].

TABLE III: Packet size comparison

	a	b	c	d	e	f
TinySec-Auth	29	8	37	26.6	1.7	3
TinySec-AE	29	12	41	28.8	7.3	10
TripleKeys	29	11	40	28.3	5.9	2.8
Proposed method	29	15	44	30.7	11.5	12.2

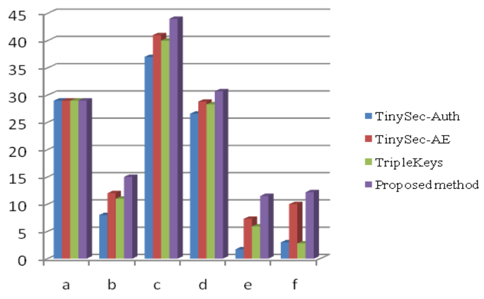

Fig. 8. Packet size comparison

The comparison of packet size overhead can also be shown graphically as in the following Fig. 8.

Here (a) = Application data, (b) = Packet Overhead, (c) = Total Size, (d) = Time to transmit (ms), (e) = Latency overhead (%), (f) = Energy overhead (%).

There is an increase in the packet size in the proposed scheme as shown in Table III. Thus there would be at most 9% increase over current TinyOS stack. However, it is to be noted that TinySec is not a complete security framework. Firstly TinySec concentrates only on Link Layer Security. Secondly there is no particular keying mechanism specified for use with TinySec. The proposed keying scheme is but a part of a complete security solution, which not only addresses the key management scheme but also concentrates in topology formation as presented in [15].

Although Triplekeys [6]-[7] claim to provide energy efficient secure system, the packet format of triple-keys available in [7] does not consider AM field. AM field should not be replaced by any other field as it leads to complexities in designing higher layer protocols as per Hamed et al. in [16].

B. Storage Overhead

A simple node stores at least three keys for encryption process throughout and the minimal keys being Ko, Kn and Kb .DCH/ RCH needs to store all the three above mentioned keys as well as Kc and Kbro. The Storage Overhead (SO) for an ordinary node is expressed as refers to “(3)”.

$$SO= [\text{Size of}((Kb *N) +Kn + Ko)] \tag{3}$$

where N is the nodes belonging to the same sector and for DCH/RCH it is expressed as refer to “(4)”.

$$SO=[\text{Sizeof}((Kb*N)+Kn+Ko+ Kc+ Kbro)] \tag{4}$$

Even if the default key size is considered to be 10 bytes with a maximum number of neighbors to be 50, the storage overhead for an ordinary node would be 60 bytes and for a CH it would be at most 90 bytes which is less than 1 KB. This overhead is acceptable for the motes available today.

V. Conclusion

In this paper a secure keying technique is proposed for the hierarchical clustered WSN topology. The keying scheme presented in this paper ensures that the entire network is never compromised even if there has been an attack in the network. This is possible because of clustering in terms of tracking and sectoring. The keying technique has an acceptable storage and computation overhead. This keying scheme is a hybrid scheme consisting of a combination of various possible keys that can be used in various WSN communication types.

Acknowledgment

We would like to give a great thank and regards to our HOD sir who gave us useful suggestion in the right direction. We would also like to give our gratitude to all our friends and all the authors of the papers and journals whom papers we have listed in the reference sections. At last but not the least we would like to give thanks to the department of CSE giving us the opportunity to work on the keying technique in wireless sensor network

References

[1] A. S. Poornima and B. B. Amberker, “Key Management Schemes for Secure Communication in Heterogeneous Sensor Networks,” *International Journal of Recent Trends in Engineering*, vol. 1, no. 1, 2009.

[2] J. P. Walters, Z. Liang, S. Weisong, and V. Choudhary, “WSN Security: A survey, chapter 17 of Security in Distributed, Grid and Pervasive Computing,” Auerbach Publications, CRC press.

[3] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, “Spins: Security protocols for sensor networks,” *Wireless Networks*, vol. 8, pp. 521 – 534, 2002.

[4] S. Zhu, S. Setia, and S. Jajodia, “LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks,” *CCS* ’03, Washington D.C., USA, New York, USA: ACM Press, pp. 62-72, 2003.

[5] W. Du, J. Deng, Y. S. Han, and, P. K. Varshney, “A key predistribution scheme for sensor networks using deployment knowledge,” *IEEE Transactions on Dependable and Secure Computing*, vol. 3, no. 1, pp. 62-77, 2006.

[6] T. A. Zia and A. Y. Zomaya, “A Secur Triple-Key Management Scheme for wireless sensor networks,” in *Proc. of INFOCOM ,25th IEEE International Conference on Computer Communications*, Barcelona, pp. 1-2, 2006 .

[7] T. Zia and A. Zomaya, “A Security Framework for Wireless Sensor Networks,” SAS 2006 – *IEEE Sensors Applications Symposium Houston*, Texas USA, pp. 7-9, 2006.

[8] M. Y. Abullah, G. Hua, and N. Alsharabi, “Sensors,” 2008, 8, 7866-7881; doi 10 .3390/58127866.

[9] Y. Li and T. Newe, “Key handling in the WSNs,” Sensors 2007, *Journal of Physics*: Conference Series 76, 012060; doi 10.1088/1742-6596/76/1/012060, 2007.

[10] B. David and N. Thomas,” Securing Wireless Sensor Networks: security Architectures,” *Journal of Networks*, vol. 3, no. 1, pp. 65-77, 2008.

[11] E. Bresson., O. Chevassut, A. Essiari, and D. Pointcheval, “Mutual authentication and Group Key Agreement for Low Power Mobile devices,” *Computer Communication*; pp. 1730-1737, 2004.

[12] S. Zhu, S. Setia, and S. Jajodia, “LEAP+: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks,” *ACM Transactions on Sensor Networks* TOSN, vol. 2, no.4, pp. 500-528, 2006.

[13] N. Gautam, W. Lee, and J. Y. Pyun, "Track-Sector Clustering for Energy Efficient Routing in Wireless Sensor Networks," cit, vol. 2, pp.116-121, *Ninth IEEE International Conference on Computer and Information Technology*, 2009.

[14] K. Chris, N. Sastry, and W. David, “TinySec: A link layer security architecture for wireless sensor networks,” in *Proc. of the Second ACM Conference on Embedded Networked Sensor Systems (Senses 2004)*, pp. 162-175, November 2004.

[15] K. Sharma, A. S. Rathor, S. R. Biradar, and M. K Ghose, “Power-efficient Routing & Increased Yield Approach for WSNs,” *International Journal on Computer Science and Engineering (IJCSE)*, vol. 02, no. 03, pp. 586-592, 2010.

[16] S. Hamed, S. Mastooreh, and D. Tassos, “Providing Transparent Security Services to Sensor Networks,” in *Proc. of IEEE* International *Conference on Communication (ICC’07)*, pp. 24-28, 2007.

Kalpana Sharma, Professor of the Department of Computer Science & Engineering at Sikkim Manipal. Institute of Technology, Mazitar, Sikkim, India since August, 1998. She did her BE from National Institute of Technology, Silchar, India and M.Tech from IIT Kharagpur, India.

Her areas of research interest are Wireless Sensor Networks, Steganography, Network & Information Security, Real Time Systems and Software Engineering. She has published a number of technical papers in various national and international journals in addition to presentation/ publication in several international/ national conferences.

M. K. Ghose is the Dean (R & D), SMIT and the Professor and Head of the Department of Computer Science & Engineering at Sikkim Manipal Institute of Technology, Mazitar, Sikkim, India since June, 2006.

His areas of research interest are Data Mining, Simulation & Modeling, Network, Sensor Network, Information Security, Optimization & Genetic Algorithm, Digital Image processing, Remote Sensing & GIS and Software Engineering. He has published a number of technical papers in various national and international journals in addition to presentation/ publication in several international / national conferences.

.

V. K. Singh, Assistant professor II, joined Sikkim Manipal Institute of Technology in July, 2010 as an Assistant Professor II.

He did his MCA from SMIT and pursuing MTECH from department of CSE, SMIT. He has published a number of technical papers in various national and international journals in addition to presentation/ publication in several international / national conferences.