Volume 2, Issue 9, September 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Network Security Management in Wireless Networks through Zero Knowledge Proof

K. VamsiRam
M.Tech [S.E]
Department of IT
SACET, Chirala(A.P.)
India

I. Bala Venkateswarlu
Associate Professor
Department of IT
SACET, Chirala(A.P.)
India

Abstract: ***Wireless Sensor Networks (WSNs) will provide an excellent opportunity to control environments. Even WSNs have lot of applications, some of them quite sensitive in nature and require full proof secured environment. The wireless security mechanism is not same as in wired networks. Because there is no user-controlling for each individual node, wireless environment, and more importantly, scarce energy resources. In this paper, we propose the 3-round zero knowledge protocol for main problem in sensor network security is that sensors are compromised once; the adversary can easily launch clone attacks by replicating the compromised node, distributing the clones throughout the network, and starting a variety of insider attacks. Previous works against clone attacks suffer from either a high communication/storage overhead or poor detection accuracy. Here, we propose a novel scheme for detecting clone attacks in sensor networks, which computes for each sensor a social fingerprint by extracting the neighbourhood characteristics and verifies the legitimacy of the originator for each message by checking the enclosed fingerprint. The fingerprint generation is based on the superimposed s-disjunct code, which incurs a very light communication and computation overhead. The fingerprint verification is conducted at both the base station and the neighbouring sensors, which ensures a high detection probability. The security and performance analysis indicate that our algorithm can identify clone attacks with a high detection probability at the cost of a low computation/communication/storage overhead. To our best knowledge, our scheme is the first to provide real-time detection of clone attacks in an effective and efficient way.***

Keywords— clone attack, man in middle attack, replay attack, 3-round zero knowledge protocol, WSN.

1. Introduction

Wireless sensor networks usually comprise a number of sensors with limited resources. Each sensor includes sensing equipment, a data processing unit, a short range radio device and a battery [1–3]. These networks have been considered for various purposes including border security, military target tracking and scientific research in dangerous environments [4–6]. Since the sensors may reside in an unattended and/or hostile environment, security is a critical issue. An adversary could easily access the wireless channel and intercept the transmitted information, or distribute false information in the network. Under such circumstances, authentication and confidentiality should be used to achieve network security. Since authentication and confidentiality protocols require a shared key between entities, key management is one of the most challenging issues in wireless sensor networks (WSNs) [4].

Wireless sensors are small and cheap devices powered by low-energy batteries, equipped with radio transceivers, and responsible for responding to physical stimuli, such as pressure, magnetism and motion, by producing radio signals. They are featured with resource (e.g., power, storage, and computation capacity) constraints and low transmission rates. Wireless sensor networks (WSNs) are collections of such wireless sensors that are deployed (e.g., using aircraft) in strategic areas to gather data about the changes in their surroundings, to report these changes to a data-processing centre (which is also called a data sink), and possibly to respond to these changes. The processing centre can be a specialized device or just one of the sensors, and its function is to analyse the collected data to determine the characteristics of the environment or to detect events. Mass-produced intelligent sensors and pervasive networking technology enable WSNs to be widely applied to various applications, ranging from military to civilian fields; examples of these applications include military surveillance, target tracking, traffic monitoring, and building safety monitoring, to list a few. Security model for wireless sensor networks. We propose a method for identifying the compromised/cloned nodes and also verifying the authenticity of sender sensor nodes in wireless sensor network with the help of 3-round zero knowledge protocol [5],[15].
The following are the most important security goals for W S N

Primary and secondary are the main types of security goals are there in Wireless Sensor Network. The primary goals are known as standard security goals such as Confidentiality, Integrity, and Authentication. The secondary goals are Data Freshness, Time Synchronization and Secure Localization. These goals are explained as follows. Primary goals are as:

A. Data Confidentiality

In sensor network the ability to conceal messages from a passive attacker is confidentiality. Due to this message communication through sensor network remains confidential. A sensor node should not show its data to the neighbours.

B. Data Authentication

The reliability of the message through identification of its origin done by authentication. Alteration of packets are basically involves in attacks of WSN Identification of senders and receivers are verified by data authentication.

C. Data Integrity

Data reliability is insured by Data integrity in sensor networks. It also haves an ability that confirm message has not been tampered with, altered or changed. Secondary goals are

D. Secure Localization

A sensor network designed to ensure faults. It accurate information related with location for identification of location fault.

2. Preparatory

A. Superimposed s-disjunct code

In this section, we introduce the basics of superimposed s-disjunct code, which incorporates social characteristics and used to generate fingerprint for each sensor node [1]. These fingerprints are subsequently used to detect clone attack. Let **X** is a m X n binary matrix. In this paper, we consider a matrix **X** with a constant column weight ω and a constant row weight λ. Then,

$$\sum_{i=1}^{m} X_{i,j} = w$$

$$\sum_{j=1}^{n} X_{i,j} = \lambda$$

Where 1 <= i <= m, 1 <= j <= n. The binary matrix **X** can be used to define a binary code word, with each column **X**j=(X1, j, X2, j,...,Xm,j)

.

Definition 1 Given two binary codewords **y** =(y1,y2, ⋯,ym)T and **z** =(z1,,z2,...,zm)T we say that **y** covers **z** if the boolean sum (logic OR operation) of **y** and **z** equals **y**, i.e. **y** ∨ **z**=**y**.

Definition 2 An mXn binary matrix X defines a superimposed code of length m,sizen, strength s (1<s<m), and list size L (1 = L = m - s), if the boolean sum of any s-subset of columns of **X** can cover no more than L columns of **X** which are not in the s-subset. This code is also called as *(s,L,m)*-code of size n.

Definition 3 A binary matrix **X** defines an s-disjunct code if and only if the boolean sum of any s-subset of columns of X does not cover any other column of X that are not in the s-subset. According to the s-disjunct characteristic of superimposed s-disjunct codes, the following important property can be employed to compute fingerprints to detect clone attacks.

Property 1 Given a superimposed s-disjunct code **X**,for any s -subset of columns of **X**, there exists at least one row in **X** that intersects all the s columns with a value 0.

Generation of a good superimposed s-disjunct code has been extensively studied in literature ([9, 10, 11, 13]). We use a superimposed s-disjunct code with constant weight in our model.

3. IMPORTANT ATTACKS IN WSN

Though there are various attacks in Wireless Sensor Networks, but certain active attacks that can be detected with our proposed model are as follows:

Clone Attack

In clone attack, an adversary may capture a sensor node and copy the cryptographic information to another node known as cloned node. Then this cloned sensor node can be installed to capture the information of the network. The adversary can also inject false information, or manipulate the information passing through cloned nodes. Continuous physical monitoring of nodes is not possible to detect potential tampering and cloning. Thus reliable and fast schemes for detection is necessary to combat these attacks [1],[13].

Man in the Middle Attack

The man-in-the-middle attack (MITM) is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection. The attacker will be able to intercept all messages exchanging between the two victims and inject new ones.

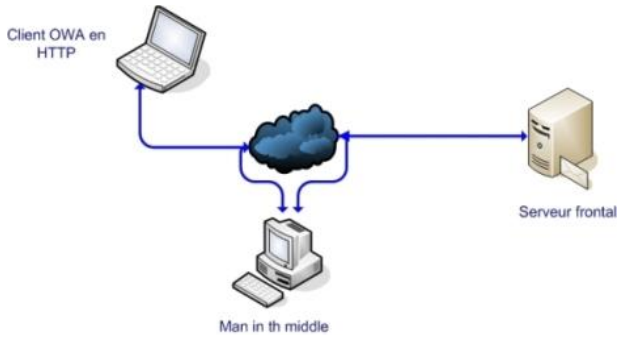


Fig1: Man in the Middle Attack

Replay Attack

A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by adversary who intercepts the data and retransmits it. This type of attack can easily overrule encryption.

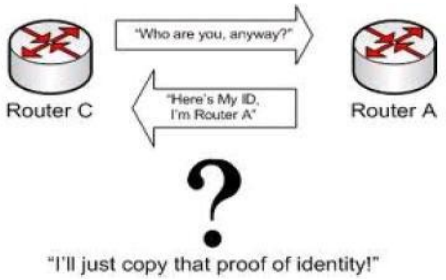


Fig2: Replay Attack

Hello flood Attack

We introduce a novel attack against sensor networks: the HELLO flood. Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbors, and a node receiving such a packet may assume that it is within (normal) radio range of the sender. This assumption may be false: a laptop-class attacker broadcasting routing or other information with large enough transmission power could convince every node in the network that the adversary is its neighbor.

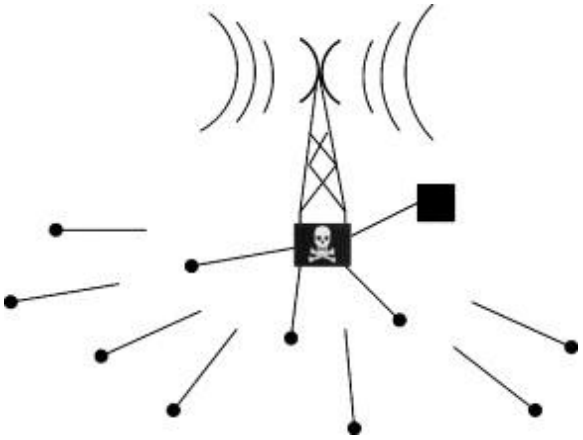


Fig3: Hello flood Attack.

4. three-round zero knowledge

The falsity of KEA2 renders vacuous the result of [11, 12] saying that there exists a negligible-error, 3-round ZK argument for WSNs security. In this section we look at recovering this result.

Prover $\bar{P}$ **Verifier** $\bar{V}$

Initial State St = (x,w,R)

((CMT,q,g**),St)** $\leftarrow \bar{P}(\varepsilon; St)$ **d←1**

$\xrightarrow{(CMT,q,g)}$

n← $|x|$

If(q,g) $\notin GL_n$ **then** d $\leftarrow$ 0 **EndIf**

$r \xrightarrow{a} Z_q^*; CH \leftarrow g^r$

$\xleftarrow{CH}$

(RSP, St) $\leftarrow \bar{P}$(CH;St)

$\xrightarrow{RSP}$

$If\ DEC_z((CMT, q, g), CH, RSP) = 0\ then$

d← 0 EndIf

A 3-round argument. The common input is x. Prover ¹P has auxiliary input w and random tape R, and maintains state St. Verifier ¹V returns boolean decision d.

We first consider the protocol of [11, 12], here called HTP. What has been lost is the proof of soundness (i.e., of negligible error). The simplest thing one could hope for is to re-prove soundness of HTP under KEA3 without modifying the protocol. However, we identify a bug in HTP that renders it unsound. This bug has nothing to do with the assumptions on which the proof of soundness was or can be based.

The bug is, however, small and easily fixed. We consider a modified protocol which we call pHTP.

We are able to show it is sound (i.e., has negligible error) under KEA3. Since we have modified the protocol we need to re-establish ZK under KEA1 as well, but this is easily done.

Arguments. We begin by recalling some definitions. An argument for a WSNs L [6] is a two-party protocol in which a polynomial-time prover tries to \convince" a polynomial-time verifier that their common input x belongs to L. In addition to x, the prover has an auxiliary input a. The protocol is a message exchange at the end of which the verifier outputs a bit indicating its decision to accept or reject. The probability (over the coin tosses of both parties) that the verifier accepts is denoted AccP;aV(x). The formal de¯nition follows.

A two-party protocol (P; V), where P and V are both polynomial time, is an argument for L with error probability ± : N ! [0; 1], if the following conditions are satisfied: Completeness, Soundness and Canonical protocols. The 3-round protocol proposed by [11, 12], which we call HTP.

5. PROPOSED MODEL

Nodes are divided into three categories; base station, cluster head and member nodes. Some arbitrary nodes are selected as cluster heads and generation of cluster heads is left to the clustering mechanism (not dealt in this work). Each cluster head knows about its member nodes, while every member node knows its cluster head. Base station stores information of all sensor nodes (including cluster heads). The base station maintains complete topological information about cluster heads and their respective members. • Base station is powerful enough and cannot be compromised like other nodes of the network [1]. • There is no communication among the member nodes.

Figure 5 describes communications using 3ZKP in the proposed model. The overview of our scheme consists of three main steps categorized into two phases

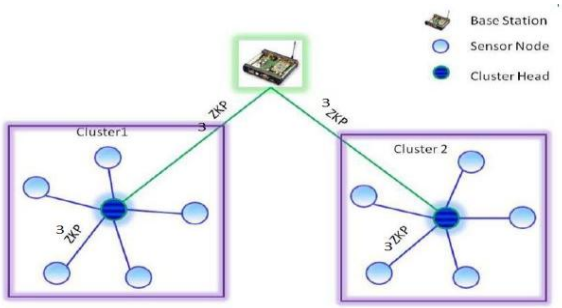


Fig4: Communications using three-round zero knowledge

Base station, cluster head and member nodes are three main nodes in this model. Mostly random nodes are considered as cluster heads. Each and every cluster head had information about its member nodes and vice versa.

The information about all sensor nodes which includes cluster heads also is stored in base station. Base station maintains all the topological information about cluster heads and their respective members by communication among member nodes is not possible.

Pre-deployment phase

For deploying the nodes in the network, we generate a unique fingerprint for each sensor node. I t add essed by combi ni ng rel at i ve nodes information through a superimposed s-disjunct code and this is preloaded in each node. Due to this each node seems unique from other one. Basically this fingerprint remains secret throughout the process.

Post-deployment Phase

A public key N generation by the base station is done after the deployment. Basically this key is used by any two nodes at a given time while communicating. Here base station is third party whereas sender node is prover and receiving node verifier. Each node is assigned a fingerprint which is used as a private key (secret key). Prover and receiver share the public key. Now from base station secret key of the prover from the base station is requested by verifier. The base station will generate a secret code $v = s2modN$ (where s is finger print of the prover and N is the public key). The value of v is given to the verifier on its request [13].Fingerprint is never shown or transmitted in the network directly during this entire communication process. By using ZKP for k times per communications verifier will continues the authentication process which includes number of verification rounds. Failure of prover for authentication of itself in any one of the k rounds, then it becomes a compromised node. For more effectiveness of protocol it must be passed through large number of rounds. The number *s* remains private within the domain of the prover. Thus makes it computationally infeasible to derive s from v given $v = s2modN$.

6. Countermeasures

Outsider attacks and link layer security the majority of outsider attacks against sensor network routing protocols can be prevented by simple link layer encryption and authentication using a globally shared key. The Sybil attack is no longer relevant because nodes are unwilling to accept even a single identity of the adversary. The majority of selective forwarding and sinkhole attacks are not possible because the adversary is prevented from joining the topology. Link layer acknowledgements can now be authenticated.

Major classes of attacks not countered by link layer encryption and authentication mechanisms are wormhole attacks and HELLO flood attacks.

Although an adversary is prevented from joining the network, nothing prevents her from using a wormhole to tunnel packets sent by legitimate nodes in one part of the network to legitimate nodes in another part to convince them they are neighbors or by amplifying an overheard broad- cast packet with sufficient power to be received by every node in the network.

An insider cannot be prevented from participating in the network, but she should only be able to do so using the identities of the nodes she has compromised. Using a globally shared key allows an insider to masquerade as any (possibly even non-existent) node. Identities must be verified. In the traditional setting, this might be done using public key cryptography, but generating and verifying digital signatures is beyond the capabilities of sensor nodes.

HELLO flood attacks

The simplest defense against HELLO flood attacks is to verify the bidirectionality of a link before taking meaningful action based on a message received over that link. However, this countermeasure is less effective when an adversary has a highly sensitive receiver as well as a powerful transmitter. Such an adversary can effectively create a wormhole to every node within range of its transmitter/receiver. Since the links between these nodes and the adversary are bidirectional, the above approach will unlikely being able to locally detect or prevent a HELLO flood? One possible solution to this problem is for every node to authenticate each of its neighbors with an identity verification protocol using a trusted base station. If the protocol sends messages in both directions over the link between the nodes, HELLO floods are prevented when the adversary only has a powerful transmitter because the protocol verifies the bidirectionality of the link.

Although this does not prevent a compromised node with a sensitive receiver and a powerful transmitter from authenticating itself to a large.

Authenticated broadcast and flooding

Since base stations are trustworthy, adversaries must not be able to spoof broadcast or flooded messages from any base station. This requires some level of asymmetry: since every node in the network can potentially be compromised, no node should be able to spoof messages from a base station, yet every node should be able to verify them. Authenticated broadcast is also useful for localized node interactions. Many protocols require nodes to broadcast HELLO messages to their neighbors. These messages should be authenticated and impossible to spoof. Proposals for authenticated broadcast intended for use in a more conventional setting either use digital signatures and/or have packet overhead that well exceed the length of typical sensor network packet. lTESLA [23] is a protocol for efficient, authenticated broadcast and flooding that uses only symmetric key cryptography and re-quires minimal packet overhead. lTESLA achieves the asymmetry necessary for authenticated broadcast and flooding by using delayed key disclosure and one-way key chains constructed with a publicly computable cryptographically secure hash function. Replay is prevented because messages authenticated with previously disclosed keys are ignored. lTESLA also requires loose time synchronization.

7. SECURITY ANALYSIS OF PROPOSED MODEL

A. Cloning Attack

Case 1: Any other existing id with same fingerprint gets used by cloned node:

As an node get compromised its clones are inserted to network which always tries to make a part of communication. Only after the verification of clone nodes they are able to communicate with other nodes Fig 5 shows how node ’6’ of cluster ’2’ is get cloned and placed in cluster ’1’ with a new id ’2’.

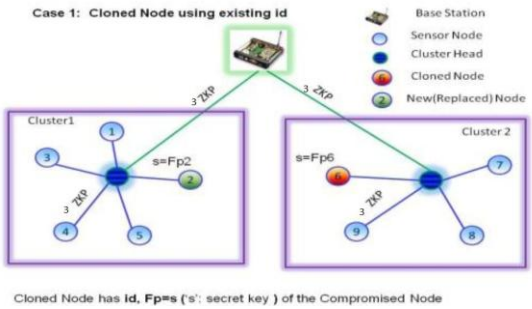
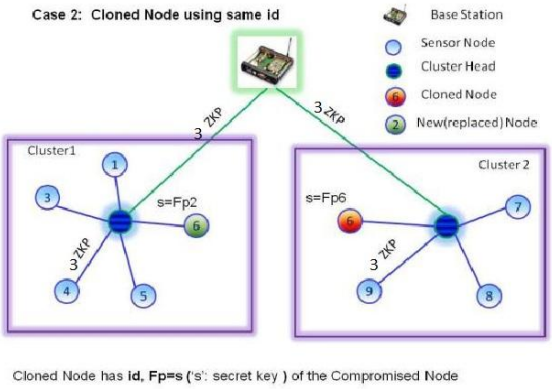


Fig5: Cloned node using existing id

Cloned node uses the fingerprints' of node '6', it fails to authenticate itself during communication through 3ZKP.

Case 2: When same id and same fingerprint used by cloned node:

If it uses the same id '6', the cluster head of cluster 1 will reject any communication as node '6' as it is not a member of cluster '1'.The base station which will detect immediately at the initiation of the communication request.



.

Fig6: Cloned Node Using same id

In our model, the finger print of a node never gets transmitted and thus intruder not haves chance to identify them. Even if the attacker tries to generate a finger print in some brute force method, it will not be able to escape the check as every time a new public key N and a new random challenge question will be used.

C. Replay Attack

In this attack, an intruder tries to replay the earlier

Communication and authenticate itself to the verifier. But, with our model verifier will be sends different values each and every time in communication, replaying earlier communication.

8. Conclusion

This paper proposed a new security model which addresses three important types of active attacks MITM attack, Clone attack and Replay attack. By using 3-round Zero knowledge protocol we implement this model. The proposed model uses finger print for each and every communication between the nodes. Thus it is easy for the administrator to identify these attacks using 3ZKP. Different types of attack there related information, different cryptographic strength and performance of the proposed model get analyzed in this system.

REFERENCES

1. Mauro Conti, Luigi Vincenzo Mancini, and Alessandro Mei, "Distributed in Wireless Sensor Networks", IEEE Transactions on Dependable and Secure Computing., vol. 8, no. 5,September/October 2011
2. L.Eschenauer and V.D.Gligor, "A Key Mauro Conti, Luigi Vincenzo Mancini, and Alessandro Mei, "Distributed Detection of Clone Attacks in Wireless Sensor Networks", IEEE Transactions on Dependable and Secure Computing., vol. 8, no. L.Eschenauer and V.D.Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. mputer and Comm. Security (CCS '02), pp. 41-47, 2002. Conf. Computer and Comm. Security (CCS '02), pp. 41
3. R. Brooks, P. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M.T. Kandemir, "On the Detection of R. Brooks, P. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M.T. Kandemir, "On the Detection of Clones in Sensor Networks Using Random Key Predistribution," IEEE Trans. Systems, Man and Clones in Sensor Networks Using Random

Key Predistribution," IEEE Trans. Systems, Man and Cybernetics, Part C: Applications and Rev., vol. 37, no. 6, pp. 1246 cs, Part C: Applications and Rev., vol. 37, no. 6, pp. 1246-1258, Nov. 2007.

4. C. Bekara, M. Laurent-Maknavicius. "A new protocol for securing wireless sensor networks against Maknavicius. "A new protocol for securing wireless sensor networks againstnodes replication attacks", In Proceedings of the 3rd IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2007. nodes replication attacks", In Proceedings of the 3rd IEEE International Con Mobile Computing, Networking and Communications (WiMob), 2007.
5. B. Parno, A. Perrig, and V.D. Gligor, "Distributed Detection of Node Replication Attacks in Sensor B. Parno, A. Perrig, and V.D. Gligor, "Distributed Detection of Node Replication Attacks in SensorNetworks," Proc. IEEE Symposium. Security and Privacy, pp. 49-63, May 2005. Networks," Proc. IEEE Symposium. Security and Privacy, pp. 49
6. Detection of Clone Attacksin Wireless Sensor Networks", IEEE Transactions on Dependable and Secure Computing., vol. 8, no. Management Scheme for Distributed Sensor Networks," Proc.
7. R. Brooks, P. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M.T. Kandemir, "On the Detection ofClones in Sensor Networks Using Random Key Predistribution," IEEE Trans. Systems, Man and Maknavicius. "A new protocol for securing wireless sensor networks againstference on Wireless and
8. Kai Xing Fang, Liu Xiuzhen, Cheng David, H. C. Du, Real-Time Detection of Clone Attacks in Wireless Sensor Networks Proceedings of the 28th International Conference on DistributedComputing Systems, 2008, Pages 3-10.
9. Joseph Binder, Hans Peter Bischof, Zero Knowledge Proofs of Identityfor Ad Hoc Wireless Networks An In-Depth Study,Technical Report, 2003. http://www.cs.rit.edu/ jsb7384/zkpsurvey.pdf
10. Klempous R.; Nikodem J.; Radosz, L.; Raus, N. ByzantineAlgorithms in Wireless Sensors Network, Wroclaw Univ. ofTechnol.,Wroclaw; Information and Automation, 2006. ICIA2006.International Conference on, 15-17 Dec. 2006, pages :319-324
11. A. J. Macula. A simple construction of d-disjunct matrices withcertain constant weights Discrete Math., 162(13):311-312, 1996
12. K. Xing, X. Cheng, L. Ma, and Q. Liang.,Superimposed Code Based Channel Assignment in Multi-radio Multi-channel Wireless Mesh Networks. In MobiCom'07, pages 15-26, 2007.
13. Md. Moniruzzaman, Md. Junaid ,Arafeen, Saugata Bose, Overviewof Wireless Sensor Networks: Detection of Cloned NodeUsing RM,LSN SET, Bloom filter and AICN Protocol and
14. Comparing H.Choi, S.Zhu, and T.Laporta.,Set: Detecting Node Clones in Sensor Networks. InSecureComm'07, 2007.
15. Goldreich, O., Micali, S., and Wigderson, Proofs That Yield Nothing But Their Validity Or All Languages in NP Have Zeroknowledge Proof Systems, Journal of the ACM, Vol. 38, No. 1,pp.691-729, 1991.
16. Tuyls, Pim T. (Mol, BE), Murray, Bruce (Eastleigh GB),Efficient Implementation of Zero Knowledge Protocols,United States NXP
17. B.V.(Eindhoven,NL)7555646,June2009,http://www.freepatentsonlin e.com/7555646.html.
18. Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Commun. SurveysTutorials, vol. 8, pp. 2–23, year 2006. (IJCSIS) International Journal of Computer Science and Information Security,Vol. 4, No. 1 & 2, 2009.
19. Siba K. Udgata, Alefiah Mubeen, Samrat L.Sabat Wireless sensor security model using zero knowledge protocol, 978-1-61284-233-2/11/$26.00 ©2011 IEEE.
20. A. G. Dyachkov and V. V. Rykov., Optimal superimposed codes and designs for Renyis Search Model. Journal of Statistical

