International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 5, No.3 (May-2016)

http://dx.doi.org/10.12785/ijcds/050303

# Ensuring Authentication and Security using Zero Knowledge Protocol for Wireless Sensor Network Applications

**Mohammad Mozumdar [1], Mehrdad Aliasgari [2], Sudheer Matta Veera Venkata [3]and Sai Santosh Renduchintala [4]**

*[1,3,4] Electrical Engineering, California State University Long Beach, Long Beach, The United States of America*
*[2] Computer Engineering and Computer Science, California State University Long Beach, Long Beach, The United States of America*

*Received 25 Jan. 2016, Revised 27 Feb. 2016, Accepted 22 Mar. 2016, Published 1 May 2016*

**Abstract:** Wireless Sensor Networks (WSNs') have turned into a prominent solution for various applications where human intervention is not possible. For the effective functioning of WSNs', the nodes must be capable enough to identify and detect malicious nodes from genuine ones. Moreover, these sensors are deployed in the network where sensitive information is transmitted between the nodes and base station. Hence, security and data authentication are the major requirements for the Wireless Sensor Networks. This paper investigates the use of an identity mechanism called Zero Knowledge Protocol (ZKP), for the authentication of sensor nodes. Our simulation results indicate that our proposed scheme ensures high security to the network with minimal overhead, minimal energy consumption, and good throughput.

**Keywords:** Wireless Sensor Networks, Zero Knowledge Protocol, Two Way Authentication, Challenge question.

## 1. Introduction

Wireless Sensor Networks (WSNs') plays a crucial role in monitoring of environmental conditions and security surveillance of various sensor node applications. Sensor nodes are deployed in the network to collect the physical parameters of the system and carry out some highly secure transmission of information between the nodes. These sensor nodes are deployed in such circumstances where there is minimal human intervention and monitoring. Since communications occur in an open environment or in hostile conditions, data authenticity and security of WSNs' is a big concern.

The data communication between nodes is carried out in an open environment and hence the possibility of physical attacks is highly likely. It is easy for an adversary to create and deploy clones in the network by replicating the cryptographic information of the legitimate nodes. The WSNs' are highly vulnerable to many other attacks such as man in the middle attacks, replay attacks, eavesdropping. Due to these conditions, the network must be capable enough to identify, detect, and protect the network from these attacks and malicious nodes. Symmetric Key encryption models such as SPINS [22], LEAP [24], and TinySec [23] are tractable in the field of WSN and can achieve data confidentiality but secret key distribution and management is a significant challenge. Hence, these algorithms poorly support data authenticity.

Public Key Cryptography (PKC) schemes are widely used and accepted to support symmetric key management as well as data authenticity. Though, the widely popular PKC scheme Rivest Shamir Adelman (RSA) technology tend to support in WSN, the performance in terms of message authenticity and integrity has been poor in sensor networks given the low clock rate, low computational power, and memory availability of the nodes. Hence, RSA algorithm can be used in authentication of nodes with a smaller public exponent e and a smaller key size, which compromises the security level of asymmetric encryption. To overcome this issue, zero knowledge protocol (ZKP) [9] is used where zero information about the secret key is exchanged between the communicating nodes. Zero knowledge proof method, implementation of identification schemes [10],

*E-mail: mohammad.mozumdar@csulb.edu, mehrdad.aliasgari@csulb.edu, sudheer1303@gmail.com, santosh.vy678@gmail.com*

and its variants have been suggested for authentication purposes in various domains.

ZKP was first introduced by Goldwasser in [9] and it is proven for its efficiency in cryptography. It can well be applied in places of authentication and secure key exchange. ZKP has extensively been used in many contexts; the usage of ZKP in Wireless sensor network is shown in [3]. In [1] ZKP is implemented for WSN considering the security attacks in WSN. It has been shown that ZKP proves efficient for the clone and man in the middle attacks. [19] Proposed ZKPs' use in WSN, an identification scheme for Base Nodes (IBN), where a group of sensor nodes cooperatively authenticates and secret key is generated based on superimposed disjunction matrices. The overall communication cost using the above process would be high and in [2] a small version of ZKP is proposed for the wireless body area network (WBAN) systems and Tiny-ZKP [3]. In this paper, we designed a new ZKP model for WSN with a flexible secret key generation at low energy consumption. Moreover, we proposed a two-way authentication technique for more secure data transfer.

The main conflict of interest of this Zero Knowledge Protocol is to reduce the computational power drastically in comparison to the previous work and also, other few protocols. This is achieved at the same time, maintaining the security level and also, overcoming the possible physical and massive attacks in any wireless network. The super-imposed matrices and digital signature mechanism are replaced using the two-way authentication implementation and RSA symmetric in generating the secret and public keys to the sensor nodes. This helps to improve the security and maintain the efficiency level of any sensor network. Here, the number of challenging questions has been increased with reducing the number of authentication rounds. So, the computation power required to implement this protocol in any wireless sensor network is reduced by a good ratio.

The rest of the paper is about the basic system model which is discussed in section 2, the proposed model of ZKP in section 3, Simulation setup, Security, and performance characteristics of the proposed model in section 4, and we conclude the paper in section 5.

## 2. SYSTEM MODEL

In the ZKP model of wireless sensor networks, there exist sensor nodes and a base station. In contrast to the sensor nodes the base station possesses much more computational power, larger memory and is often connected to better energy source like power grids. The duty of the base station is to accomplish the tasks of routing, node configuration, and gather-sensed data from the sensor nodes in wireless sensor networks.

Zero Knowledge Protocol is an authentication mechanism in which the secret key is not at all shared between the nodes, but it is the responsibility of the verifier to authenticate the prover using the protocol for the successful data transfer. In our model, the sender node acts as a prover and the receiver node acts as a verifier. In ZKP, it is the role of prover to authenticate itself as a legitimate node for data transfer, and it is the role of verifier to authenticate the prover by asking challenge questions. In the proposed model, the base station before receiving any information also authenticates the verifier.

The base station maintains complete topological information such as node IDs', and secret keys of all nodes.

Fig. 1 depicts the architecture of the system model. Some of the trust assumptions of the base station are as follows:

1. The base station is trustworthy, powerful and cannot be compromised.
2. The base station is responsible for the generation and distribution of secret keys to all the nodes.
3. A legitimate node does not perform any malicious activity unless there is an influence of an adversary on it.

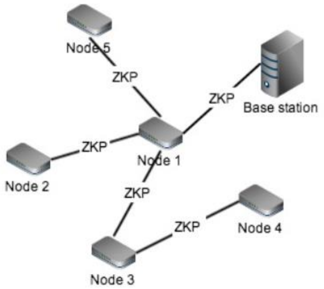

Figure 1. Architecture of Zero Knowledge Protocol mode

## 3. PREPARE YOUR PAPER BEFORE STYLING

The proposed ZKP model can be classified into two categories. They are pre-deployment phase, and post-deployment phase.

## A. Pre-deployment Phase

The base station (BS) is the heart of the system and is considered to be reliable for the operation of the network. As mentioned earlier, the BS possesses more computational power, and larger memory; the concept of RSA is introduced in generation of secret key utilizing the BS computational abilities. The generation of secret key is carried out in the pre-deployment phase without any overhead to the network. The initial setup is carried out by choosing two random large prime numbers p and q to yield n (public key), where n is the product of p and q of infeasible factorization. Then φ(n) which is the product of (p-1) and (q-1) is calculated. The BS takes the responsibility of assigning node IDs' and code numbers. In order to do this, each node is assigned with a node ID j and a code number $C_j$ ($1 < C_j < \varphi(n)$). For instance, code number of node ID 1 is $C_1$ and node ID 2 is $C_2$ and so on. In our model, the generation of secret key is carried out based on the neighboring nodes information. The BS calculates distance between nodes by using X, Y dimensions of each node and its surrounding nodes and randomly chooses the neighboring node which falls in the threshold distance margin.

→ *Illustration of secret key generation:*

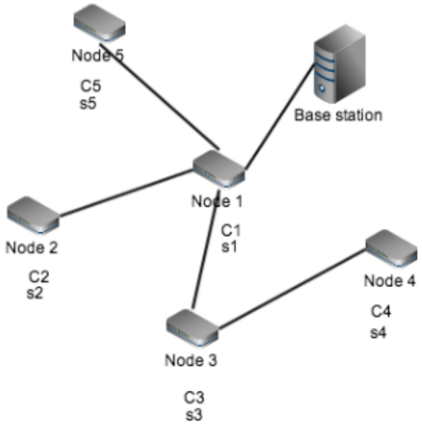

Figure 2. Illustration of secret key generation

For example, in the Fig. 2, Secret key of node 2 is to be calculated. In order to calculate secret key of node 2, the neighboring nodes of node 2 are determined using their positions by the base station. The neighboring nodes of node 2 are node 1, node 3, and node 6. Out of these three neighboring nodes, anyone node is selected randomly by the BS. Let's assume node 1 is selected. Now, code number of node 1 is chosen such that

$$1<C_1< \varphi(n), \text{ and}$$
$$\gcd(C_1,\varphi(n)) = 1$$

Where φ(n) = (p-1)*(q-1) and p,q are two large prime numbers.

Now, secret key of node 2 is calculated as shown below:

$$(S_2) = C_1^{-1} \bmod \varphi(n) \quad \text{i.e. } S_2 * C_1 \bmod \varphi(n) = 1$$

Where, $S_2$ is the secret key of node 2, $C_1$ is the code number of node 1.

As you can observe from Eq. 3 that the neighboring nodes code number is used in the calculation of secret key of that particular node. This provides extra security to the system and protects the network from different attacks like clone attacks, replay attacks, and man in the middle attacks. In the similar procedure, secret key of all nodes in the network are calculated, stored, and distributed to the respective nodes by the base station.

In [1] super-imposed disjunction matrices were used to calculate the unique fingerprint for each node. A unique fingerprint for each sensor node is computed by incorporating the neighboring information through superimposed S-disjunct code before the deployment of nodes. This unique fingerprint is used as a secret key and it varies for different nodes. In the proposed mechanism, the storage and computational processing involved in superimposed large S-disjunct matrices is reduced. The secret key is calculated by using a code number and modular function, which is computationally simpler with respect to the large disjunct matrices. Thus the security of the system is based on the infeasible factorization of public key (n) to yield p and q and also due to the properties of inverse modulo.

## B. Post-deployment Phase

After the generation of secret key and node deployment, the nodes will communicate with each other. It is the responsibility of receiver (verifier) node to authenticate the sender (prover) node in order to accept data and it is the responsibility of sender node to prove itself as a legitimate node for the secure data transfer. Zero Knowledge Protocol does this authentication procedure and the communicating nodes for data authentication share public key n. Before we go into the authentication process, let us recollect different keys generated by the base station, prover node, and verifier node respectively. The entire two-way authentication mechanism technique is clearly shown in the Fig 3 below.

*Keys generated by the Base Station*

- n: Public key generated based on the product of two large prime numbers p and q.
- S: Secret key associated with a node. Every node has a separate secret key.
- $V_P$: Protocol key of the prover generated on the basis of secret key of the prover.

*Keys generated by the Prover*

- r: Random value generated for each round.
- X: Value generated based on the value 'r'.
- Y: Value generated based on the verifier challenge e.

*Keys generated by the Verifier*

- $V_V$: Protocol key of the verifier generated on the basis of secret key of the verifier.
- Val1: Value generated after receiving the challenge value from the prover.
- Val2: Value generated after receiving the value $V_P$ from the base station.

The authentication process is initiated when the prover P chooses a random number r and calculates $X = r^2$ mod N. The prover sends X to the verifier as a first step of authentication process. The verifier requests for the prover protocol key $V_P$ from the base station. Now, the BS sends the protocol key of the prover only after it successfully authenticates the verifier. This is called two-way authentication. In two-way authentication, the BS calculates the protocol key of the verifier $S_V^2$ mod n by using the resources it has in calculating the secret key of the verifier. The BS now asks for the protocol key ($V_V$) of the verifier and compares the value it calculated with that of the protocol key ($V_V$), which was sent by the verifier. If these are equal, the BS authenticates the verifier and sends the protocol key ($V_P = S_P^2$ mod n) to the verifier where $S_P$ is the secret key of the prover.

The verifier now chooses a random challenge question e (e = 0, 1, 2, 3, 4) and asks the prover to calculate $Y = rS_P^e$ mod n where r is the random number chosen by the prover, $S_P$ is the secret key of the prover, and n is the public key generated by the BS. The prover calculates Y and sends it to the verifier as a response to its challenge question e. The verifier will now compute Val1 = $Y^2$ mod n and Val2 = $XV_P^e$ mod n. If both Val1 and Val2 are equal, the prover is said to be authenticated for that particular round. The verifier can run this protocol K number of times until it believes the prover to be legitimate.

We know Val1 = $Y^2$ mod N (where $Y = rS_P^e$ mod N). The prover calculates the value of Y by using its secret key. Hence, the Val1 is evaluated with the secret key of the prover $S_P$. Now Val2 = $XV_P^e$ mod N (where $V_P = S_P^2$ mod N). The protocol key of the prover $V_P$ is calculated with the secret key evaluated by the base station for that particular node ID. Hence the Val2 is generated with the secret key calculated by the BS. As the BS is assumed to be a trusted third party and if Val1 equal to Val2 for K number of rounds, it implies that the prover is a genuine node.

The above explained authentication process can be reframed in the following steps:

1. The prover P chooses a random number r and calculates X.
2. The prover P then sends X to the verifier.
3. The verifier requests for the provers' protocol key $V_P$ from the base station.
4. The BS calculates $S_V^2$ mod n and compares this value with $V_V$. If both are equal, it authenticates the verifier.
5. Now, the BS sends the protocol key $V_P$(Prover Protocol Key) to the verifier.
6. The verifier chooses a random challenge question e and asks the prover for $Y = rS_P^e$ mod n.
7. The prover calculates Y and sends it to the verifier as a response to the challenge question e.
8. The verifier now calculates Val1 (= $Y^2$ mod n) and Val2 (= $XV_P^e$ mod n). If Val1 and Val2 are equal, the prover is said to be authenticated for that particular round. Val1 and Val2 can be equal if the secret key of the prover and secret key calculated by the BS for that node ID is identical.

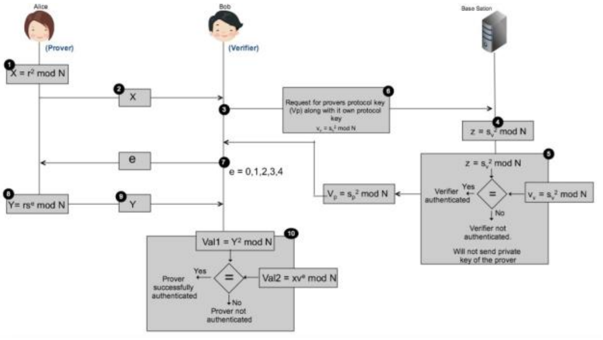

Figure 3. Proposed Zero Knowledge Authentication Mechanism

In [2], when e has 2 values the optimal number of rounds were 10, which makes the probability of successful authentication by a malicious node to $(1/2)^{10}$. In our proposed model, we increased the security of the system by increasing the challenge questions and reducing the number of rounds. In our case with e = 5, we achieved the same security with 4 rounds which makes the probability of successful authentication by a malicious node to $(1/5)^4$, simultaneously reducing computational costs. After successful authentication in all rounds, the data transfer takes place between the nodes where they exchange information.

*Example of ZKP mechanism:*

*Pre-Deployment Phase:*

Step 1: Consider two large prime numbers p,q. For our convenience

$$p = 31, q = 53$$

Step 2: Calculate the public key n, where $n = p*q$

$$n = 31*53 = 1643$$

Step 3: Calculate $\varphi(n)$, where $\varphi(n) = (p-1)*(q-1)$

$$\varphi(n) = (31-1)*(53-1) = 1560$$

Step 4: Calculate the secret key of the nodes. Lets calculate secret key of node 6 with node 1 as its neighboring node selected randomly by the base station. In order to calculate secret key of node 6, the code number of node 1 is to be determined.

$$C_1 = 1193$$

$$S_6 = C_1^{-1} \bmod \varphi(n) = 17$$

So, $C_1$ is a co-prime to $\varphi(n)$ and $S_6*C_1 \bmod \varphi(n)$ must be 1 i.e. $17*1193 \bmod 1560 = 1$

Step 5: In the similar way secret key of all nodes is calculated by the base station in the above process and is assigned to the respective nodes along with storing in its memory.

Step 6: Calculate secret key of node 4 with node 3 as its neighboring node. In order to calculate secret key of node 4, the code number of node 3 is to be determined.

$$C_3 = 877$$

$$S_4 = C_3^{-1} \bmod \varphi(n) = 973$$

So, $C_3$ is a co-prime to $\varphi(n)$ and $S_4*C_3 \bmod \varphi(n)$ must be 1 i.e. $973*877 \bmod 1560 = 1$.

*Post-Deployment Phase:*

In our example shown in Fig 4, let us consider node 6 to be the prover and node 4 to be the verifier.

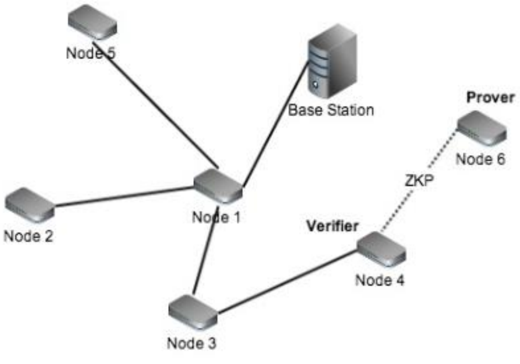

Figure 4. Zero Knowledge Protocol Authentication mechanism

Step 1: Node 6 calculates X and sends it to node 4, where $X = r^2 \bmod n$

Let $r = 235$ i.e. $X = 235^2 \bmod 1643 = 1006$

Step 2: Verifier (Node 4) asks the base station for the provers'(Node 6) protocol key.

Verifier Protocol Key $V_4 = S_4^2 \bmod n = 973^2 \bmod 1643 = 361$

The BS compares the protocol key of the verifier with that of the value stored in its memory. If they are equal, then verifier node 4 is authenticated and the BS sends the protocol key of the prover node 6 to the verifier as requested.

Prover Protocol Key $V_6 = S_6^2 \bmod n = 17^2 \bmod 1643 = 289$

Step 3: Verifier asks the challenge question e to prover and asks him to calculate Y, where $Y = rS_P^e \bmod n$.

Let e = 1 in this case.

$$Y = 235*17^1 \bmod 1643 = 709$$

Step 4: The verifier now calculates Val1 and Val2, where $Val1 = Y^2 \bmod n$ and $Val2 = XV_P^e \bmod n$

$$Val1 = 709^2 \bmod 1643 = 1566$$

$$Val2 = 1006*289^1 \bmod 1643 = 1566$$

Step 5: As both Val1 and Val2 are equal, node 6 is authenticated for that particular round

Step 6: This process is repeated for K number of times with different challenge questions e until the verifier gets satisfied with the authenticity of the prover, thus ensuring extra security.

*Observations:*

- Val1 and Val2 are equal only if the secret key of the prover is equal to the secret key generated by the base station for the prover node.
- In pre-deployment phase, the base station assigns secret key to all the nodes. So, a malicious node impersonating itself to be a legitimate node cannot falsify the verifier as the secret key of the prover would be different from that of the base station and hence Val1 and Val2 cannot be equal.
- An eavesdropper replicating the legitimate prover cryptographic information and communicating with the verifier node cannot break the ZKP protocol due to the added security. Even if the malicious node authenticates itself to be a legitimate node for one particular round, the authentication takes place for K rounds with different challenge questions thus protecting the system from false nodes.

## 4. Performance Analysis

In this section, the performance of proposed ZKP is analyzed in terms of security and efficiency.

### A. Security Analysis

In the proposed ZKP model, the authentication process is carried out based on the fact that no secret key is exchanged between the two communicating nodes as well as the base station. Security of the system depends on the infeasible derivation of secret key from the protocol key ($V_P$ or $V_V$). The secret key cannot be computed from the protocol key due to the infeasible factorization of public key N, and impracticable nature to deduce inverse square root modulo. The security of the system is more enhanced by increasing the challenge questions and optimizing the number of rounds, thus protecting the system from various physical attacks. Due to the secured ZKP mechanism, an adversary neither gets access to the network nor can it extract crucial information from the network. The physical attacks, which are limited in our proposed model, are discussed below:

#### a) Clone Attack

In the clone attack, attacker clones the legitimate node and duplicates all the cryptographic information of it. The possibility of these attacks can be of two types. First is when the clone node uses a different node ID with the same cryptographic information of that of the genuine node. The ZKP authentication would fail in this case and data transfer does not take place as the node ID stored in the base station for that secret key is different to that of the clone node ID. Hence, node ID and secret key mismatch occurs. Second is when the clone node uses the same node ID of that of genuine node with a different secret key. The authentication mechanism fails and data transfer halts between the nodes as the node ID and secret node ID based on the neighboring nodes by BS is different from the clone nodes' secret key.

For example, a clone node with node ID 2 clones node 6 and thus all the cryptographic information of node 6 i.e. secret key of node 6 is copied by the node 2. The clone node will not be able to authenticate itself as a legitimate node because the secret key associated with node ID 2 stored in the base station is different to that of node ID 6. Thus, an adversary cannot prove to the verifier that it's a genuine node, please see Fig. 5

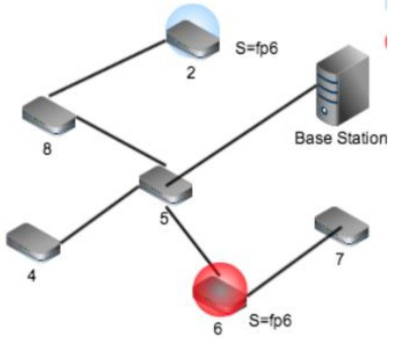

Figure 5. Clone node with different node ID, but with same secret key

Similarly, when node 6 is cloned with same node ID but with a different secret key, the authentication is halted due to secret key and node ID mismatch (Fig. 6).

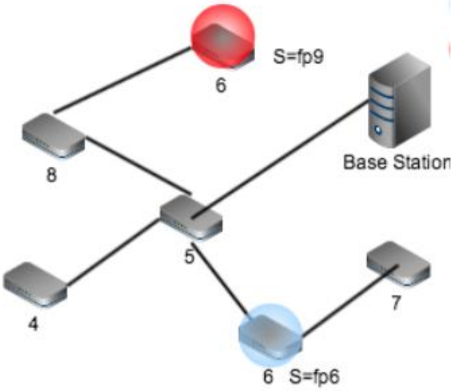

Figure 6. Clone node with different secret key, but with same node ID

#### b) Replay Attack

In the replay attack, an adversary captures messages and sensitive information from the originator and re sends them into the network pretending to be a legitimate node. The proposed ZKP protocol however detects these attacks by multiple random challenge questions. Due to the random questions for number of rounds, an adversary cannot capture data. As the adversary cannot generate valid answers to all the challenge questions, the authentication fails eventually.

#### c) Man in the Middle Attack

The MIMT attack is an active form of eavesdropping in which the attacker makes independent connections between the prover and verifier. An attacker may modify and relay messages between them. However, in our proposed model the attacker cannot make its own independent connection between prover and verifier, as it won't be able to get any data about the secret key from the communication between the prover and verifier.

*d) Interleaving Attack*

In this attack, the adversary guesses the network pattern and tries to communicate with the genuine node using the previous protocol information. In the proposed method, due to the high complex nature of the ZKP model the probability of an attacker knowing about the previous protocol information is negligible. Even if an adversary manages to get the previous protocol information, it cannot guess the challenge questions imposed by the verifier as these are chosen randomly for different rounds. With an indefinite pattern the adversary will eventually fail to authenticate it.

*e) Confidentiality Attack*

In this attack, an adversary pretends to be a verifier and capture all the private and sensitive information from the trusted party. In the proposed model with two-way authentication, this attack is limited as the verifier has to first authenticate itself to the BS before receiving any private information of the prover.

### *B. Simulation Setup and Efficiency Analysis*

Efficiency is an important parameter for successful implementation of a model. In the proposed model, the efficiency is determined based on the security, communication overhead and throughput. Simulation was carried out in Network Simulator 2. We used a wireless channel with two-ray ground radio propagation comprising of 18 mobile nodes. The maximum topography of X and Y dimensions of each node was set to 1216 and 743 respectively.

*Implementation and Methodology:*

*Software Specifications:*

- Operating System: LINUX Ubuntu
- Simulator: Network Simulator 2
- Language: Tcl/Tk
- Protocol: AODV Routing Protocol

*Hardware Specifications:*

- Processor Type: Intel(R) Core(TM) i5
- Processor Speed: 2.40GHz
- RAM: 8GB

*a) Security and Communication Overhead*

Security of the system is based on the number of challenge questions. As the number of challenge questions increases, security of the system should increase for efficient operation. In the proposed model, we achieved optimal security of the protocol with an increase in the number of challenge questions and less number of rounds(refer to Fig. 7).

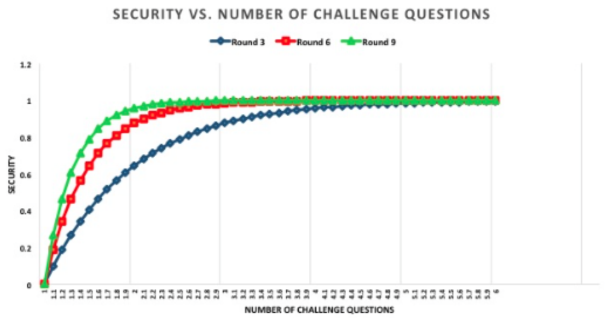

Figure 7. No. Of challenge questions VS Security

In Fig. 8, the communication overhead for different protocols is compared and we can observe that the overhead requirement for the proposed ZKP model is least when compared to other protocols. The reason for this is the minimal key size and less number of rounds.

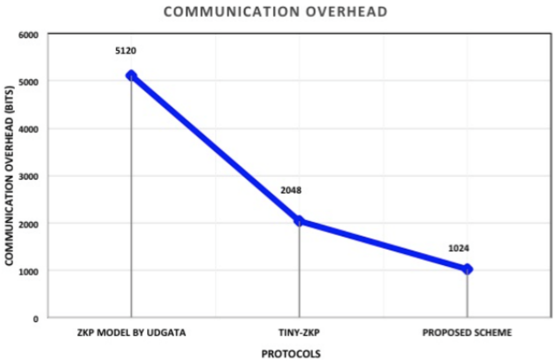

Figure 8. Comparison of different protocols with Communication Overhead

*b) Throughput and Packet Delivery Ratio*

The throughput in wireless networks is defined as the rate of successful message delivery over a network node usually measured in bits/second. In Fig 9, throughput of the network is illustrated.

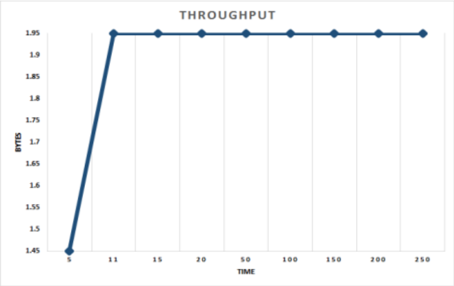

Figure 9. Illustration of throughput in our network model

Packet delivery ratio is defined as the ratio of packets that are successfully delivered to the destination compared to the number of packets that have been sent out by the sender. Fig. 10 shows the packet delivery ratio.

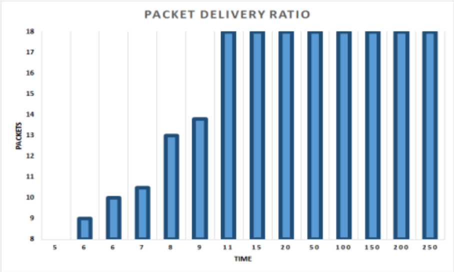

Figure 10. Illustration of Packet Delivery Ratio

### c) *Success probability of malicious authentication*

In ZKP, security of the system increases with the increase in number of rounds. Thus the probability of successful authentication of an attacker decreases considerably with the increase in challenge questions and rounds. In Fig. 11, we can observe that there is an increase in security (step manner) with the increase in number of rounds. The success probability of the proposed scheme is shown below, see (11).

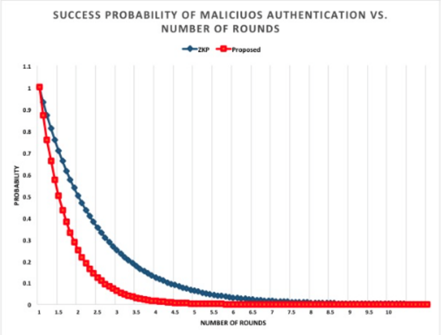

Figure 11. Illustration of Success Probability of malicious authentication in ZKP and our proposed ZKP model

### d) *Execution Time*

The execution time of the proposed ZKP is discussed here. The execution time in our proposed ZKP model is slightly higher than the Tiny ZKP. This slight increase in the execution time is due to the introduction of higher value of challenge questions i.e. e = 2, 3, 4. The computation time increase due to the 3rd and 4th order computations, which further increase the execution time. Fig. 12 shows the execution time of different protocols.

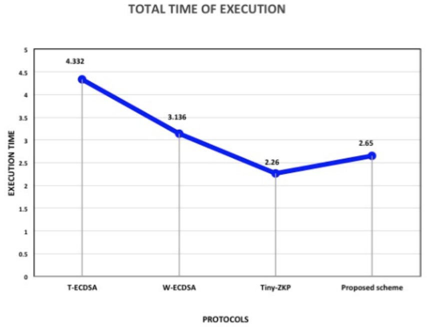

Figure 12. Comparison of Execution times of different protocols

## 5. CONCLUSION

In this paper, we proposed an efficient ZKP model which not only authenticates the prover, but also the verifier which is called two way authentication model. With two-way authentication, the network ensures added security, as the base station does not transfer sensitive data to the false verifier, thus avoiding confidentiality attack. We achieved high security with minimal communication overhead by optimizing the number of rounds and increasing the challenge questions. Our ZKP model performs better in terms of memory, security, and communication overhead than in [2]. We also analyzed various physical attacks, strengths and performance of the protocol. Our future research interests include minimizing the energy consumption, reducing the execution time and making it more power efficient.

## REFERENCES

[1] Venugopal, K.R., and Patnaik, "Authentication in Wireless Sensor Networks using Zero Knowledge Protocol", ICIP 2011, CCIS 157, pp. 416-421, 2011. Springer-Verlag Berlin Heidelberg.

[2] Udgata, S.K., Mubeen, A., Sabat, S.L., "Wireless Sensor Network Security model using Zero Knowledge Protocol" Proceedings of ICC, IEEE International Conference, 2011, pages 1-5.

[3] Ma, L., Ge, Y., "TinyZKP: A Lightweight Authentication Scheme Based on Zero Knowledge Proof for Wireless Body Area", Wireless Pers Commun DOI 10.1007/s11277-013-1555-4, Springer Science+Business Media New York 2013.

[4] Fang, K.X., Xiuzhen, L., David, C., Du, H. C. “Real Time Detection of Clone Attacks in Wireless Sensor Networks”, Proceedings of the 28th International Conference on Distributed Computting Systems, 2008, Pages 3-10.

[5] Komninos, N., Vergados, D., Douligeris, C., “Detecting Unauthorized and Compromised Nodes in Mobile Adhoc” Network-sJournal of Ad Hoc Networks, Volume 5, Issue 3, April 2007, Pages: 289-298.

[6] Ryszard, K., Jan, N., Lukasz, R., Norbert, R. “Adaptive misbehavior Detection in Wireless Sensors Network based on Local Community Agreement”, 14th Annual IEEE International Conference and Workshops on the Engineering of Computer Based Systems, ECBS 2007, Page(s): 153-160.

[7] Loannis, K., Dimitriou, T., and Frieling, F.C. “Towards Intrusion Detection in Wireless Sensor Networks”, In Proc. of the 13th European Wireless Conference, 2007.

[8] Binder, J., and Bischof, H., “Zero Knowledge Proofs of Identity for Ad Hoc Wireless Networks an In Depth Study”, Technical Report, 2003. http://www.cs.rit.edu/jsb7384/zkp-survey.pdf.

[9] Goldwasser, S., Micali, S., Rackoff, “The Knowledge Complexity of Interactive Proof Systems”, SIAM J. Computing 18, 186-208 (1989).

[10] Feige, U., Fiat, A., Shami, J., “Zero Knowledge Proofs of Identity”, Cryptology 1, 77-94 (1988).

[11] Choi, H., Zhu, S., and Laporta, T., “Set: Detecting Node Clones in Sensor Networks”, InSecureComm’07, 2007.

[12] Goldreich, O., Micali, S., and Wigderson, “Proofs that yield Nothing but their Validity or All Languages in NP have Zero Knowledge Proof Systems”, Journal of the ACM, Vol. 38, No. 1, pp.691-729, 1991.

[13] Tuyls, Pim T. (Mol, BE), Murray, Bruce (Eastleigh, GB), ‘’Efficient Implementation of Zero Knowledge Protocols”, United States NXP B.V. (Eindhoven, NL) 7555646, June 2009, http://www.freepatentsonline.com/7555646.html.

[14] Guillou, L.C., Quisquater, J., “A Practical Zero Knowledge Protocol Fitted to Security Microprocessor Minimizing both Transmission and Memory”, In: GAlunter, C.G. (ed.) EUROCRYPT 1988. LNCS, Vol. 330, pp. 123-128. Springer, Heidelberg (1988).

[15] Malan, D.J., Wells, M., Smith, M.D., “A Public Key Infrastructure for Key Distribution in TinyOS Based Elliptic Curve Cryptography”, In: 1st International IEEE Conference on Sensor and Ad Hoc Communications and Networks, pp. 71-80. IEEE Press, New York (2004).

[16] Shnayder, V., Hempstead, M., Chen, B., Allen, G.W., Welsh, M., “Simulating the Power Consumption of Large Scale Sensor Network Applications”, J. ACM transactions on sensor networks 7, 188-200 (2010).

[17] Cheng, M.Q., (2009) “A Zero Knowledge Proof of Digital Signature Scheme Based on the Elliptic Curve Cryptosystem”, InProc. of 3rd International symposium on Intelligent Information Technology(pp. 612-615), Nanchang, China: IEEE.

[18] Hashim, M., Kumar, S.G., and Sreekumar, A., “Authentication in Wireless Sensor Networks using Zero Knowledge Protocol”, ICIP 2011, CCIS 157, pp. 416-421, 2011, Springer-Verlag, Berlin Heidelberg 2011.

[19] Anshul, D., Roy, S.S., “A ZKP Based Identification for Base Nodes in Wireless Sensor Networks”, In: 2005 ACM Symposium on Applied Computing, pp. 319-323. ACM Press, New York (2005).

[20] Md. Moniruzzaman, Md. Arafeen, J., Bose, S., “Overview of Wireless Sensor Networks: Detection of Cloned node using RM, LSN, SET, Bloom Filter, and AICN Protocol.

[21] Krontiris, I., Benenson, Z., Giannetsos, T., Frieling, F.C., and Dimitriou, T., “Cooperative Intrusion Detection in Wireless Sensor Networks”, InProc. EWSN 09. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 263-278.

[22] Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J., “SPINS: Security Protocol in Network Sensor”, InProc. of 7th Annual International Conference on Mobile Computing and Networks, July, 2001.

[23] Karlof, C., Sastry, N., and Wagner, D., “Tinysec: A Link Layer Security Architecture for Wireless Sensor Networks”, Sensys, 2004, pp. 162-175.

[24] Zhu, S., Setia, S., and S. Jagodia, “Efficient Security Mechanisms for Large Scale Distributed Sensor Networks”, TOSN, Vol. 2, 2006.

**Dr. Mohammad Mozumdar** received the Ph.D. degree in electronics and communication engineering from the Politecnico di Torino, Italy. His novel ideas of model-based design for sensor networks made profound impact on engineering and industrial communities and have been published in book chapters, renowned journals, conference proceedings, major scientific magazines, and also translated in several different languages. He is a Tenure Track Faculty with the Electrical Engineering Department, California State University at Long Beach, and an ex-post-doctor from the University of California, Berkeley. His research interests include methodologies and tools for embedded system design, in particular, in the domain of sensor networks; energy efficient building management and control system design; cloud computing; cyber physical system; and methodology for the design of distributed embedded systems subject to high real time, safety and reliability constraints.

**Dr. Mehrdad Aliasgari** received his Ph.D. from University of Notre Dame in Computer Science and Engineering. His research area is computer security and applied cryptography particularly privacy-preserving computation. He is an assistant professor at the department of Computer Engineering and Computer Science in California State University, Long Beach.

**Sudheer Matta Veera Venkata** received his Master's in Electrical Engineering at California State University Long Beach. He works as a Network Engineer at Cisco Systems, TX. He expertise in LAN switching, IP routing, server load balancing, network security and firewall.

**Sai Santosh Renduchintala** received his Master's in Electrical Engineering at California State University Long Beach. He works as a Linux Build Engineer at TD Bank, NJ. He expertise in Shell scripting, UNIX administration, Build Java Applications, IP routing and sensor networks.