A Novel ZKP Approach for Security in Wireless Sensor Network

Mukesh Kansari
M.Tech(Scholar)
Department of computer Science and Engineering
RCET , Bhilai(C.G.), India

Mrs. Shikha Pandey
Reader
Department of computer Science and Engineering
RCET , Bhilai(C.G.), India

***Abstract*— Wireless Sensor Networks (WSNs) recommend an outstanding possibility to check environments in the field of information/computer Technologies, and have a lot of attractive applications, some of which are quite perceptive in nature and require full proof secured location. The aim of this paper is to discuss secure routing in Wireless Sensor networks. I have made an endeavor to present an analysis on the security of wireless sensor networks. Previous works against clone attacks suffer from either a high communication/storage overhead or reduced detection accuracy. We propose a method for revealing of scattered sensor cloning attack and use of novel zero knowledge protocol (NZKP) for verifying the authenticity of the sender sensor nodes or zones. The cloning attack is addressed by attaching a unique fingerprint to each sensor node that depends on the set of nearest nodes and itself. The fingerprint is commencing of among every message to secret in the sensor node. The ZKP is used to construct certain non communication of critical cryptographic information in the wireless network in order to avoid clone attack, MITM attack, replay attack,** distributed attack, **denial of service (DoS) and phishing attack etc. The security and performance analysis indicate that our RSA algorithm can identify clone attacks with a high detection probability at the cost of a low computation/communication/storage overhead. RSA is an algorithm for public-key cryptography that is based on the presumed complexity of factoring large integers, the factoring problem. RSA stand meant for Ron Rivest, Adi Shamir as well as Leonard Adleman,A user of RSA create and after that publish the manufactured goods of two big prime numbers, alongside with an secondary value, as their at liberty key.the fingerprint generation is based on the prime number system, which provides a very glow communication and working away overhead. To our best knowledge, our scheme is the first to provide real-time detection of clone attacks in an efficient and well-organized way.**

Keywords— ***DOS attack, MITM attack, clone attack, threat, novel zero knowledge protocol, WSN, etc.***

I. INTRODUCTION

A Wireless Sensor Network is a special type of network that consist of distributed, low-power, small size devices using sensors to cooperatively collect information through infrastructure less ad-hoc wireless network [24]. They are envisioned to play an important role in a wide variety of areas ranging from critical military surveillance applications to building security monitoring in the near future [25]. It shares some commonalities with a typical computer network, but also exhibits many characteristics which are unique to it. The security services in a Wireless Sensor Network should protect the information communicated over the network and the resources from attacks and misbehavior of nodes. Wireless sensors are little and inexpensive 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. Advances in technology have made it possible to develop sensor nodes which are compact and in expensive.[8] They are mounted with a variety of sensors and are wireless enabled. Once sensor nodes have been deployed, there will be minimal manual intervention and monitoring. But, when nodes are deployed in a hostile environment and there is no manual monitoring, it creates a security concern to a nodes may be subjected to various physical attacks. The network must be able to autonomously detect, tolerate, and/or avoid these attacks. One important physical attack is the introduction of cloned nodes into the network. When commodity hardware and operating systems are used, it is easy for an adversary to capture legitimate nodes, make clones by copying the cryptographic information, and deploying these clones back into the network. These clones may even be selectively reprogrammed to subvert the network. Individual sensor node contains a light weight processor, cheap hardware components, less memory. Because of these constraints, general-purpose security protocols are hardly appropriate. Public key cryptography is based on RSA approach. The energy consumption and computational latency makes RSA inappropriate for sensor network applications. Security algorithms that are designed specifically for sensor networks are found to be more suitable [1],[2],[3]. The goal of this paper is to develop a 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 zero knowledge protocol [4],[5]. In this paper, we address some of the special security threats and attacks in WSNs. We propose a scheme for detection of distributed sensor cloning attack and use of new name as a novel zero knowledge protocol (NZKP) for verifying the authenticity of the sender sensor nodes. The cloning attack is addressed by

attaching a unique fingerprint to each node that depends on the set of neighboring nodes and itself.

II. ATTACKS

An **attack** is one in which a prohibited modify of the system is attempt. This may possibly contain, for example, the modification of transmitted or stored data, or the creation of new data stream. Though there are various attacks in Wireless Sensor Networks, but sure active attacks that can be detect with our future project model.

III. 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:

A.clone attack

In clone attack, a challenger may confine a sensor node and fake the cryptographic information to another node or zones as known as cloned node or zone. Then this cloned sensor node or zone can be installing to detain the information of the network. The challenger can also insert false or fake information, or influence the information passing through cloned nodes or zones. Incessant corporeal monitoring of nodes is not possible to detect possible tamper and clone in the network. Thus consistent and rapid schemes for detection are necessary to conflict these attacks.[1,6].

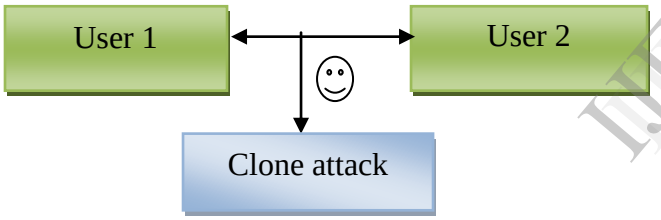

Fig. 3.1 clone attack system

B.Man in the Middle Attack

The man in the middle attack is one in which the attacker intercept communication/massage in a public key substitute and subsequently retransmits them, substitute his individual public key for the request one, accordingly with the purpose of the two creative party still come out to be communicating with each other .The attack get its given name from the ball game where two people try to throw a ball directly to each other while one person in between them attempts to catch it. In a man in the middle attack, the interloper uses a program to facilitate show to be the server to the client and come out to be the client to the server. The attack may be used basically to expand access to the message or information, and enable the attacker to transform the message or information to before retransmitting it.[8,20]

Fig. 3.2 MITM attack system

B. Replay Attack

A replay attack is a variety of network attack in which a suitable data communication is unkindly or unfairly frequent or late. This is approved elsewhere also by the inventor or by challenger who intercepts the data/information and retransmits it. This type of attack can with no trouble rule against encryption.[8,20,23]

IV. NOVEL ZERO KNOWLEDGE PROTOCOL

The functions do communicate between data or information to verifier a type's ''novel zero knowledge protocol'' Prover do a type to intensive methodology problem to offer or create and they are solve to function with many in verifier. and they show's to following diagram's.

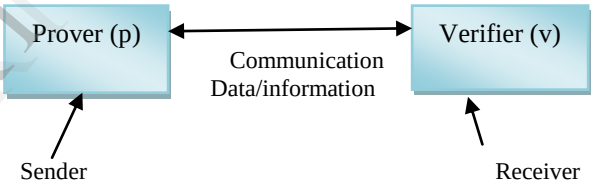

Fig. 4.1 communication between p and v

A function in this type as do prover (p) sender with prover navel zero knowledge protocol. As a protocol to middle with verifier and prover do responses and this are protocols less Bandwidth, less computational power and less memory to support.[8,20,23]

Another authentication method from equal easy and WSN do for best suitable. We are known in this project in ZKP to new name to call NZKP. They have from proper in NZKP and this methodology for example to given in WSN an authentication. We use RSA algorithm to support in this methodology.[8,23] We have given clone attacks to process provided security direct by prime number system and by removing s-disjoint code method and we are coding randomly prime number processes. Here first generate topology as given prime number randomly.

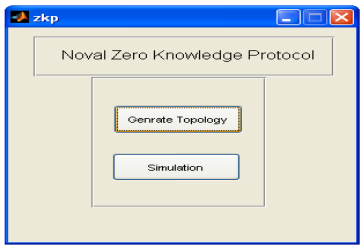

Fig.4.2 runs to project novel zero knowledge protocol

A. Basic Mechanism of Zero Knowledge Protocol

The use and implementation of ZKP in systems and devices that have restricted computational resource are described in[5].The prover P and the verifier V may use some numeric value, referred as the secret number of the prover P. Conventionally, the prover will offer a computational intensive mathematical problem, and the verifier will ask for one of the many possible solutions to the problem. If the prover knows critical information relating to the solution, it provides any one of the requested available solutions on demand. If the prover does not know the critical information, it is computationally infeasible for it to always provide the requested solution to the verifier. Usually, ZKP rely on some hard mathematical problems such as the factorisation of integers or the discrete logarithm problem.[8,20].

V. PROPOSED MODEL

We have divided to three parts on the nodes. They are directly a prime number. The overview of our scheme consists of three main steps categorized into three phases such as Pre-deployment Phase, Unique fingerprint generate for node, Post-deployment Phase.

A. Pre-deployment Phase

This phase generate a topology for all sensor node is compute by incorporate the neighborhood in sequence all the way through a prime number such as 2,5,3,13,etc.and is preloaded in each node. The fingerprint allows each node to be abnormal from others and this fingerprint will remain a secret and acts as the private key for the sensor node during the communication process. **RSA** be an algorithm for public-key cryptography with the purpose of is or base on the assumed complexity of factoring large integers, the factoring problem. A user of RSA creates and then publishes the invention of two large prime numbers, along with a additional value, as their public key. The prime factors must be kept secret in information or data. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can believably decode the message.

B.Unique fingerprint generate

This part to define generating a unique fingerprint and the base station is implicit to be conscious of the topology of the network communicates in each sensor nodes or zones. Before deployment, the base station computes the finger print for each node in the network. For every node, base station finds

(1) Base station
(2) Cluster head
(3) Member nodal

This is a main point which secret information by one cluster head and second cluster head from transfer. The base station maintains complete topological information about cluster heads and their respective members, Here this type's whole function will easily to powerful network node we show from to diagram from following:-

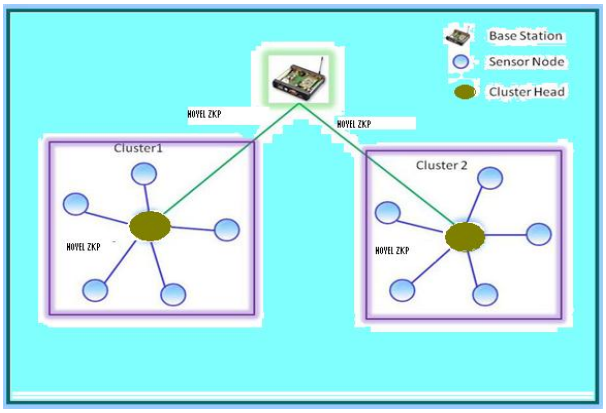

Fig. 5.1model for used to Communications in different nodes

VI. EXPERIMENTAL SETUP

MATLAB has been used to conduct the experiments and verify the proposed model. Here generate a fingerprints its zone information such as cluster head and member nodes. RSA involves a **public key** and a **private key.** The public key can be known by each one and is used for encrypting communication or Messages. Messages or communication encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. Here is an example of RSA encryption and decryption. The parameters used here are artificially small.

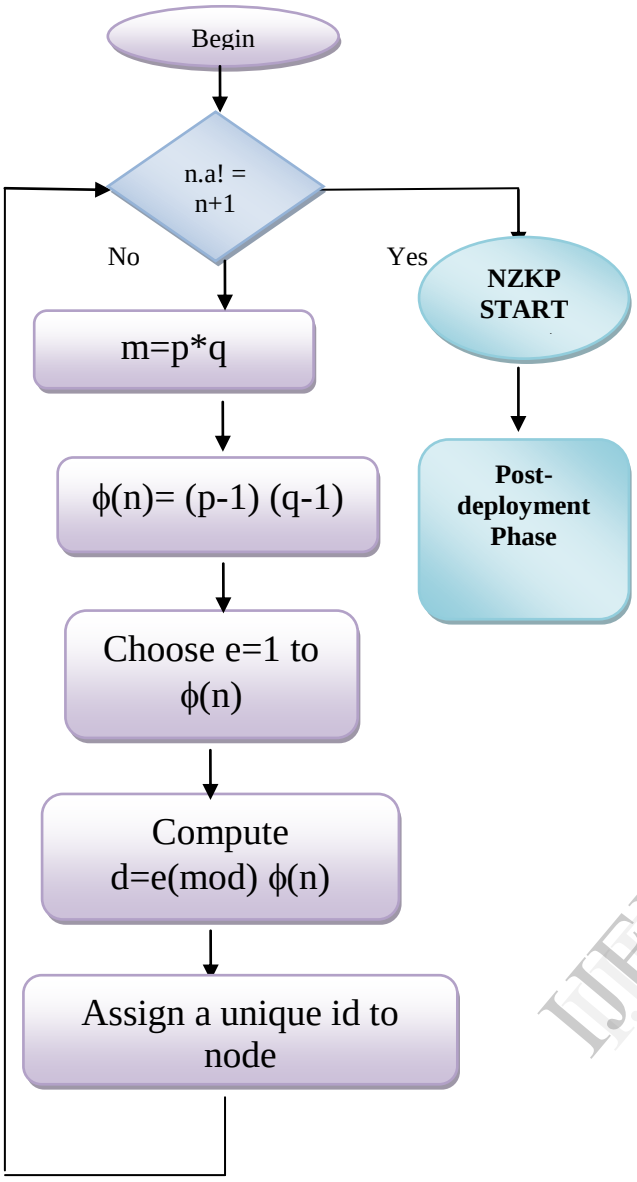

Fig. 6.1 key generate a fingerprint for each nod

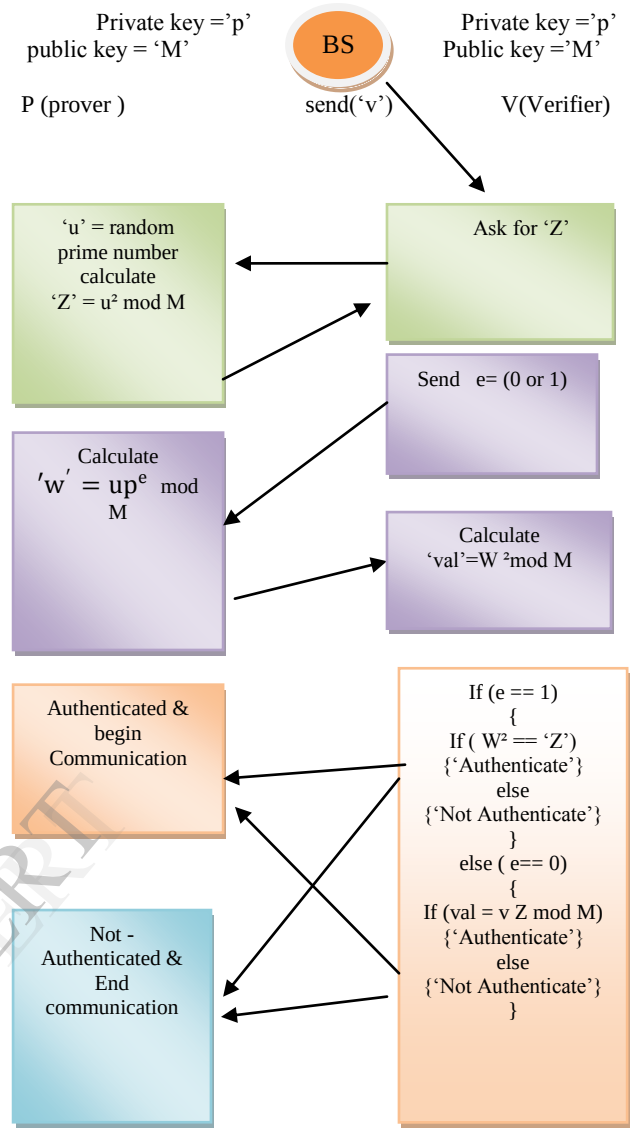

Fig. 6.2 Implementation of ZKP in our Proposed Scheme

B.Post-deployment Phase

In this deployment phase, a public key M (multiplication of large prime numbers) is generated by the base station which will be shared among any two nodes that will be communicating at a given time. throughout the communication the sender node acts as the prover while the receiver node acts as the verifier. The base station acts as the trust third party each node is assigned a fingerprint which is used as a private key (secret key). The public key M is shared among the sender (prover) and the receiver (verifier). Verifier will appeal for the top secret key in of the prover from the base station. The base station will generate a top secret code 'Z' = u² mod M (where u is finger print of the prover and M is the public key). The value of v is given to the verifier on its demand. For the duration of the entire communication process the secret i.e. fingerprint is not at all exposed or transmit in the set of connections straight.

To be well-organized, the protocol is traditionally accepted out over a realistically big prime number of round. Respectively in a surround give verifier (V) a rising scope of self-assurance that prover(P) knows the correct prime number u. The number *u* remains secret information surrounded by the area of the prover. Since M is a product of at least two large primes unknown to verifier(v) , it is really easier said than done to factories(number), and thus makes it computationally infeasible to obtain u from Z given $Z = u^2 mod M$.

Phase 1: The first phase or stage is defined to prover P choose the randomly prime numbers calculates $u^2 mod M$ and transmit to the verifier V.

Phase 2: The second phase or stage is distinct the verifier V at the moment chooses one of two questions to ask the prover P and The verifier V be able to ask either for the value of the product $'w' = up^e$ mod M, or for the value of u (fingerprint) that the prover have currently favored. This is generally

performed by V, sending a bit *e* to P, signifying its preference of the problem, referred to as the dispute, such that the prover P has to provide the answer.

Phase 3: The second phase or stage is defining the prover P provides $'w' = up^e \mod M$ as request and the verifier check the outcome as follows. If the confront is for e=1, the verifier expects to have received up mod M. The verifier cannot assume any information about p from this, because u is a random prime number not known to V. Therefore, the verifier check $u^2 \mod M$, which should be $(up \bmod M)^2 \bmod M$ is the same as $u^2 * p^2 \bmod M$. The verifier received e from P in Phase 1 of this round, and gets *v* from the trust third party.

If the challenge is for $e = 0$, the verifier expects to have received u, and checks that its square matches the value of u mod M provided in Phase 1. All the above three Phases are discussed in Fig.6.2.

The complete protocol requires execution of a adequate prime number of rounds to satisfy V that it is communicating with P, and not an impressionist. Each round requires the use of a new value of randomly prime number u. The protocol also requires that the response to a challenge be provided within a time limit such that it becomes computationally infeasible for an impressionist to answer to the challenge by using some creature power method.

VII. Security Analysis of in this Model

The security analysis in clone attack to define in four cases in our proposed model using a NZKP.

The cluster 1,the sensor node here define a prime number such as 2.3.5.7 and 11 .
The cluster 2, the sensor nodes here define a prime number such as 13,17,19,23 and29.
The cluster 1, cluster head define prime number 31 and cluster 2, cluster head define prime number 37.The base station defines prime number 41.

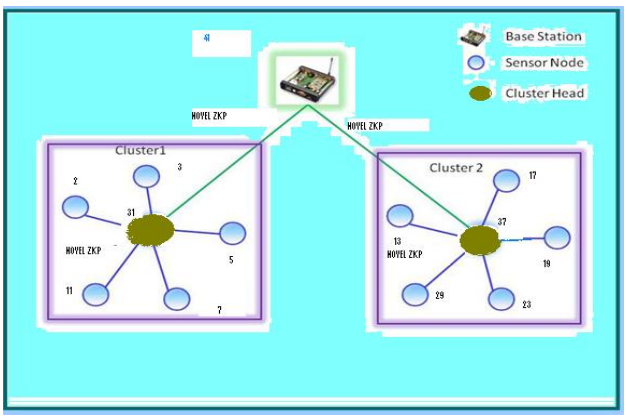

Fig. 7. 1 Clone attack security analysis

Case 1: When the cloned node uses any other existing id with same finger print

When the cloned node uses any other existing id with same finger print When a node is compromised and cloned, its clones are launched in the network and try to take part in the communication. The cloned nodes will not be able to communicate with any other node until and unless it is verified (by cluster head if it is a cloned member node and base station if it is a cloned cluster head). This situation is explain in Figure 7.2 such a node '13' of cluster '2' is cloned and placed in cluster '1' with a new id '5'. Since the cloned node uses the finger print 'g' of node '13', it will fail to authenticate itself during communication through NZKP.

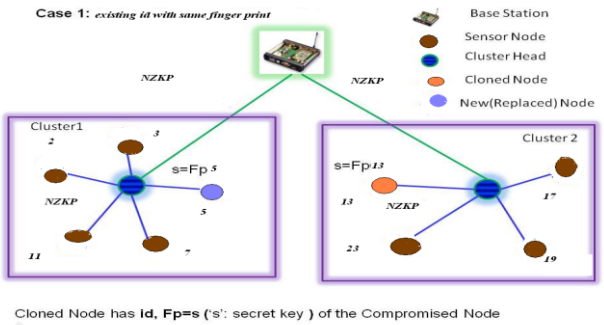

Fig. 7.2 Clone attack existing id with same finger print

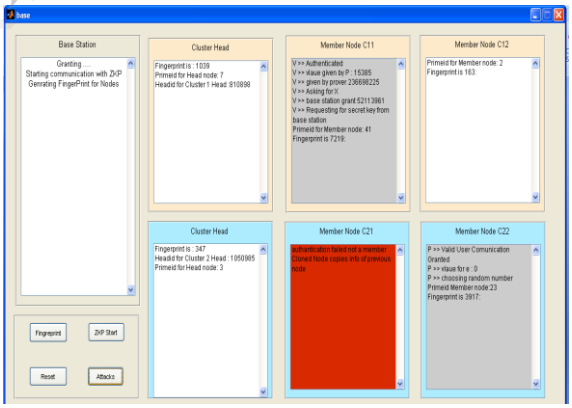

Fig. 7.3 existing id with same finger print

Case 2: When the cloned node uses same id with same finger print

When the cloned node uses same id with same finger print If it uses the same id '13', the cluster head of cluster 1 will reject any communication as node '13' as it is not a member of cluster '1'. The base station which will detect immediately at the initiation of the communication request. This scenario is depicted in Figure 7.4

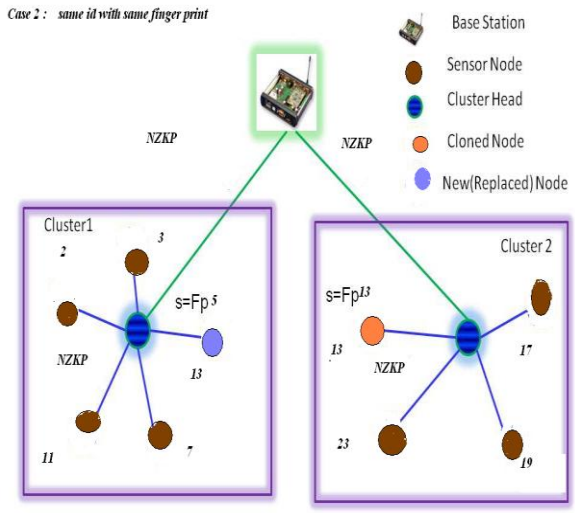

Fig. 7.4 same id with same finger print

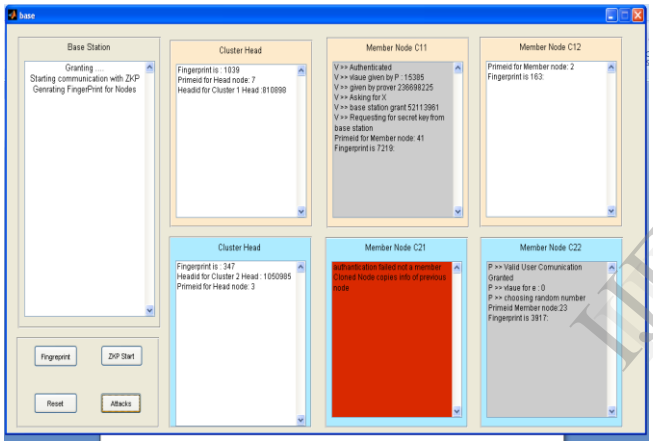

Fig. 7.5 same id with same finger print

Case 3: When cloned node uses existing id with a different finger print

The cloned node having some existing id can always be detected by the neighboring nodes (cluster heads) as the secret finger print of the cloned node will not match with the finger print possessed by the neighbors. The following finger to show cluster1, cluster2 and base station. The node provided Prime number cluster1 such as 2,3,5,7,9,11 and cluster2 such as 13, 17,19,23,29 and cluster1 member node 31,and cluster2 member node 37.

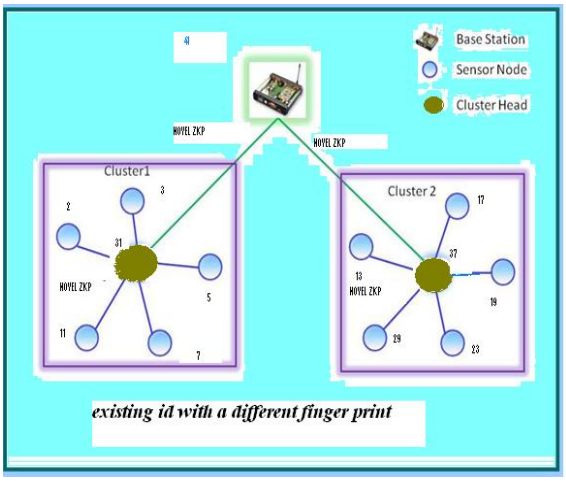

Fig. 7.6 existing id with a different finger print

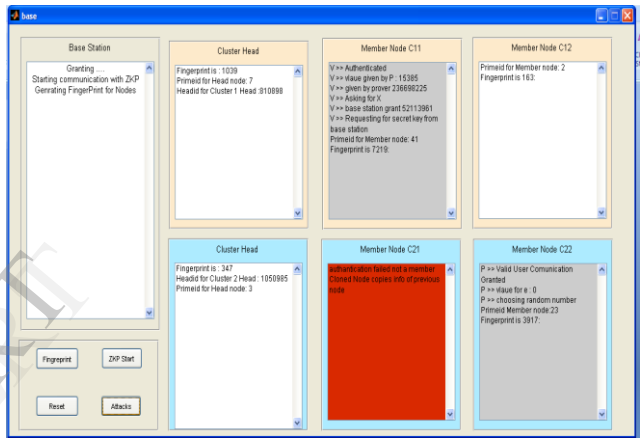

Fig. 7.7 existing id with a different finger print

Case 4: When a cloned node behaves as a cluster head

The cluster heads communicate with base station which has all information about the nodes. The base station becomes the verifier and poses the challenge question to the cloned cluster head and detects the cloning attack through NZKP.

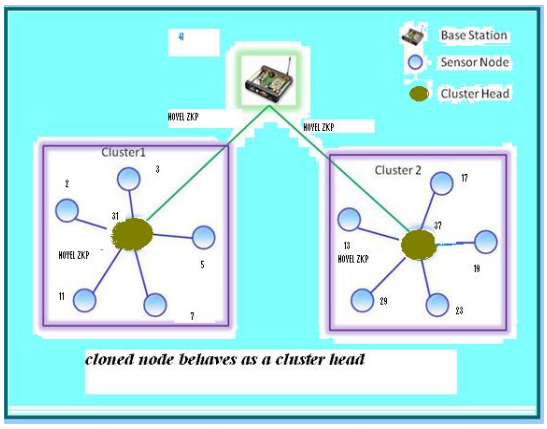

Fig. 7.8 cloned node behaves as a cluster head

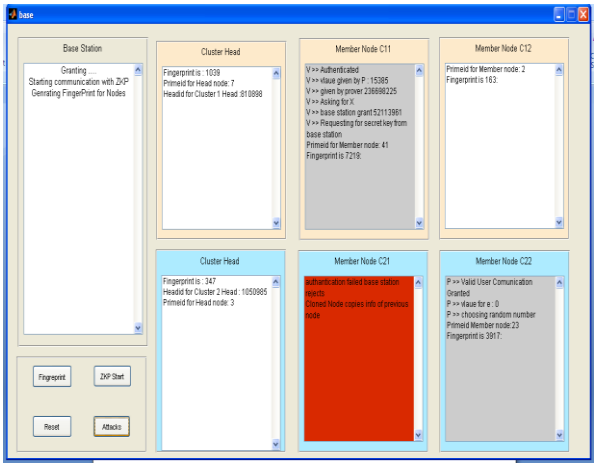

Fig.7.9 behaves as a cluster head

VIII. CONCLUSION

Wireless Sensor networks have become promising future to many applications.In the absence of enough security, deployment of sensor networks is vulnerable to variety of attacks. Overall security for wireless sensor networks is very hard to develop due to the limited resources of the sensors.Sensor network security will always be a field in which much work needs to be done. Current research in sensor network security is mostly built on a trusted environment however there are several research challenges remain unanswered before we can trust on sensor networks. In this paper we have discussed threat models and unique security issues faced by wireless sensor networks. In WSNs, there are still some challenges that are to be addressed. the cryptographic strength of NZKP is based on few hard to solve problems. The one which we have used in our scheme is based on the problem of factoring large prime numbers that are product of two or more large (hundreds of bits) primes. The values of the public key also changes with every announcement, creation it more complicated for the attacker to guess it. in this paper, we proposed a new security model to address one important attack namely clone attack.We used the concept of novel zero knowledge protocol which ensure non-transmission of vital information between the prover and verifier.

We recommend extending our project work in future to detect the passive and active attacks.Evaluate performance in real time using new methodology in novel zero network protocol.We propose to expand our work to distinguish the passive attacks also and estimate performance in real time using TinyOS and Tossim

REFERENCES

[1] 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 Distributed Computing Systems, 2008, Pages 3-10.

[2] Nikos Komninos, Dimitris Vergados, Christos Douligeris, *Detecting Unauthorized and Compromised Nodes in Mobile Adhoc Networks* Journal of Ad Hoc Networks, Volume 5, Issue 3, April 2007, Pages: 289-298 .

[3] Klempous Ryszard, Nikodem Jan, Radosz Lukasz, Raus Norbert, *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, 2007, Page(s):153-160.

[4] Joseph Binder, Hans Peter Bischof, *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.

[5] 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

[6] H. Choi, S. Zhu, and T. Laporta. Set: Detecting node clones in sensor networks. In *SecureComm'07*, 2007.

[7] B. Parno, A. Perrig, and V. Gligor. Distributed etection of node replication attacks in sensor networks. In *SP '05*, pages 49–63, 2005.

[8] Kai Siba K. Udgata, Alefiah Mubeen,Department of Computer & Information Sciences,Samrat L. Sabat,School of Physics,University of Hyderabad,Hyderabad, "Wireless Sensor Network Security model using Zero Knowledge Protocol",Proceedings of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2011

[9] M. Subramanya Bhat* and J.T. Devaraju Associate Professor, Department of Electronic Science Wireless Sensor Networks: A Performance Study of IEEE 802.15.4 Standard Volume 3, No. 5, Sept-Oct 2012 International Journal of Advanced Research in Computer Science

[10] Amit Chaudhary and Bhumica Verma Computer Science & Engineering, Modern College of Engineering &Technology, India ,"Prosperity, Vulnerabilities and Security Threats in WSN" Volume 3, No. 5, Sept-Oct 2012 International Journal of Advanced Research in Computer Science

[11] Krontiris Ioannis, Tassos Dimitriou and Felix C. Freiling, *Towards Intrusion detection In Wireless Sensor Networks*, In Proc. of the 13th European Wireless Conference, 2007.

[12] A. A. Taleb, Dhiraj K. Pradhan and T. Kocak *A Technique to Identify and Substitute Faulty Nodes in Wireless Sensor Networks* Proceedings of the 2009 Third International Conference on Sensor Technologies and Applications, 2009, Pages: 346-351

[13] Klempous R.; Nikodem J.; Radosz, L.; Raus, N. *Byzantine Algorithms in Wireless Sensors Network*, Wroclaw Univ. of Technol., Wroclaw; Information and Automation, 2006. ICIA 2006. International Conference on, 15-17 Dec. 2006, pages :319-324

[14] I. Krontiris, Z. Benenson, T. Giannetsos, F. C. Freiling, and T. Dimitriou, *Cooperative Intrusion Detection in Wireless Sensor Networks*, in Proc. EWSN'09. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 263-278.

[15] A. G. Dyachkov and V. V. Rykov., *Optimal superimposed codes and designs for Renyis Search Model*. Journal of Statistical Planning and Inference, 100(2):281-302, 2002.

[16] A. J. Macula. *,A simple construction of d-disjunct matrices with certain constant weights* Discrete Math., 162(13):311-312, 1996.

[17]. E. Shi, and A. Perrig, "Designing secure sensor networks", Journal of IEEE Wireless Communications, Vol. 11, Issue 6, Dec. 2004 pgs 38-43.

[18] Md. Moniruzzaman, Md. Junaid Arafeen, Saugata Bose, *Overview of Wireless Sensor Networks: Detection of Cloned Node Using RM, LSN, SET, Bloom filter and AICN Protocol and Comparing*

[19] 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.

[20] K.Radhika, B.Mahesh ," Detection of Various Attacks in Wireless Sensor Networks Using Zero Knowledge Protocol", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

[21] Manish P.Gangawane , *M.E. I.T. Student, M.I.T.M. Indore, RGPVB,* " Implementation Of Zero Knowledge Protocol In Wireless Sensor Network for Identification Of Various Attacks ", nternational Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 8, August 2012)

[22] K.Y.Maheswari, A.Satchidanandam ane,Dept of CSE, RRS College of Engineering and Technology, Patancheru, Medak, A.P, India," a

proficient approach towards wireless sensor network safety model",International Journal of Computer and Electronics Research [Volume 2, Issue 3, June 2013]

[23] Vishal Parbat, Tushar Manikrao,Nitesh Tayade, Sushila Aghav, Department of Computer Science, Pune University, Pune-38," Zero Knowledge Protocol to design Security Model for threats in WSN" , International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 2,Mar-Apr 2012, pp.1533-1537

[24]. Tan f Akylidiz, Weliain S U, yogesh sankarasubramaniam and eradal caryici. "A survey on Sensor Networks" IEEE Communication Magazine, august 2002.

[25]. Yuanzhu Peter Chen Arthur L. Liestman Jiangchuan Liu. "Energy-Efficient Data Aggregation Hierarchy for Wireless Sensor Networks" Proceedings of the 2nd Int'l Conf. on Quality of Service in Heterogeneous Wired/Wireless Networks August 2005.