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

Access Control Schemes & its Security Measurements in Wireless Sensor Networks: A Survey

Raj Kumar[1], Sameer Kumar Singh[2]
CSED, NIT Hamirpur (H.P.), INDIA

Ritesh Kumar[1]
E&CED, P.K.I.T.M.Mathura (U.P.), INDIA

Abstract— **Nodes in the Wireless Sensor Network may be lost due to either depletion of battery power or malicious attacks. So it is inevitable to insert a new node for the extension of life time of Sensor Networks. A lot of researchers proposed their works towards this arena that is how to make our Sensor Networks secure. Basically making our Sensor Networks secure, there is a mechanism of Access Control in Sensor Networks. Through the implementation of Access Control we could make our Sensor Networks secure in against of various malicious attacks as well as to save unnecessarily exhaustion of Sensor Networks' resources. This paper addresses the existing Access Control schemes over Wireless Sensor Networks.**
In this paper, we presents existing Access Control Schemes over Wireless Sensor Networks and discuss how those protocols make safe our Sensor Networks against various types of security threats..

Keywords— **Wireless Sensor Networks, Security Vulnerabilities, Access Control Schemes, Security Threats.**

I. INTRODUCTION

Wireless Sensor Networks is a type of Ad-hoc Network, which refers thousands or millions of sensor nodes are, deployed in an attendant territory that sense data and send it to the fixed node called Sink. It has several unique characteristics, which include hostile environment, limited resources, in-network processing and application-specific architectures etc. The constituents of Sensor Network, sensor nodes also having limited memory, low processing capability and limited battery power. As a consequence, a lot of vulnerabilities might be possible under this circumstance. Even if, there is possibility of making unnecessarily exhaustion of resources of this Sensor Networks.

A potential use of Wireless Sensor Networks in civilian and non-civilian area like battle field surveillances, traffics monitoring, home security etc [5]. But due to scarcity of security of Sensor Network, this became impractical in our real life implementation. That's why; it attracts a lot of interests in the area of making Access Control Protocols in Wireless Sensor Networks. These Access Control Protocols make our Sensor Network secure with preventing unnecessarily depletion of resources of Sensor Networks. Many researchers contribute their job in making of Access Control Protocols in WSNs.

Here we presents the survey of those existing Access Control Protocols in WSNs and make fruitful to new comer for complete analysis of those protocols. Along with we here also describe the how these protocols makes our WSNs secure against malicious attacks.

The remainder of this paper is organized as follows Section-II details the background. Section-III reviews different existing attacks in the Sensor network. Section-IV presents existing Access Control Protocols in WSNs. Section-V presents defensive measurements of schemes and Section-VI presents the performances of existing proposed schemes. Last section concludes this paper.

II. BACKGROUND

A. Security Vulnerabilities in WSNs

The characteristics of Wireless Sensor Networks makes a lot of vulnerabilities and prone to several security threats [5]. We are making distinction between physical and technological vulnerabilities as-

Physical vulnerabilities

The low temper resistant and hostile deployment of sensor nodes make easy to compromise. These compromised sensor nodes attracts various link to passive eavesdropping to active interfering in Sensor Networks. The thousands to millions sensor nodes deployment also demands simple, flexible and scalable Access Control protocols.

Technological vulnerabilities

The technological vulnerabilities in Wireless Sensor Networks are followings [9]-

Energy: Only source of energy consumption are in the process of listening, sensing and receiving, but making exhaustion of energy in some other tasks producing vulnerabilities.

Computation: The computational engine is only awarded with simple one not complex one.

Memory: The limited memory of Sensor node does not attracts complicated algorithm.

Transmission Range: The communication range of sensor nodes is low due to technically and by the need to conserve energy.

Wireless Communication: Only wireless nature makes unsuitable to traditional wired Access Control protocols.

B. Wireless Sensor Networks Architecture

The Wireless Sensor Networks refers a network of thousands or millions of small, cheap sensor nodes, deploy in event region or near about event region and makes sensing data related to events and send data to a fixed node called Sink (Base Station). The layout of Wireless Sensor Networks are-

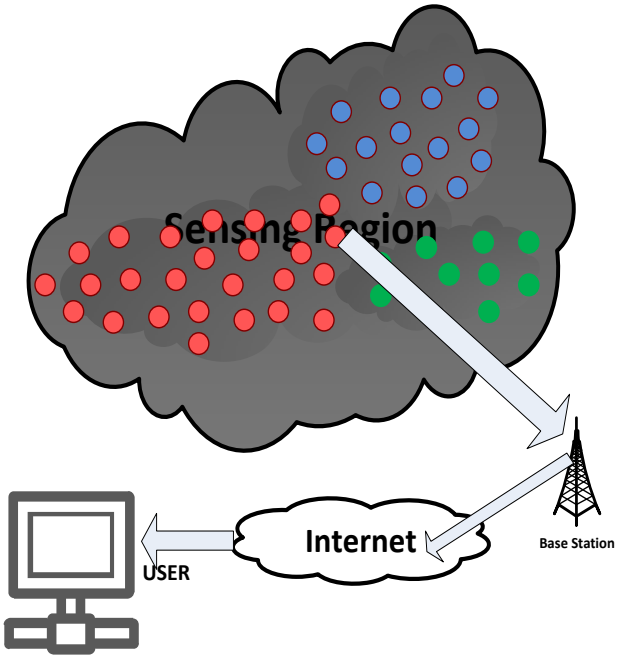


Figure 1

III. Review of Attacks

It is seen that generally Wireless Sensor Networks is setup in an unattendent area i.e. lack of infrastructures. So there is a possibility of vulnerabilities by an adversary in Sensor Networks. Adversary can directly deploy malicious nodes to eavesdrop messages sent out or received by normal nodes or even inject false reports to disrupt the network functionalities [1] as the implementation of Eavesdropping attack in sensor networks. The Sybil Attack a particularly harmful attack in sensor networks where a malicious node behaves as if it were a larger number of nodes, for example by impersonating other nodes or simply by claiming false identities. The malicious node may be deployed directly by adversaries or just a compromised one. In the Figure 2(a) the pictorial view of Sybil attack is shown where an adversary node AD behaves like impersonated node. From the perspective of node A, node AD appears as node B, from the perspective of node C as node E. It is very dangerous to our sensor networks. The wormhole attack makes a tunnel in the sensor networks by two nodes (either compromised legitimate node or malicious node deployed by attacker) and produces great concerns in sensor networks as making two remote nodes as very near to each other as depicted in figure 2(b). It makes a great harm to routing protocols in sensor networks as well as challenging the whole system. It confuses entire sensor networks. Node replication is direct replication of legitimate node o throughout the sensor networks. It makes a lot of clones of a single or a set of compromised legitimate nodes. It is shown in figure 2(c). A lot of another security threats present in our sensor networks but a very few are discussed here only.

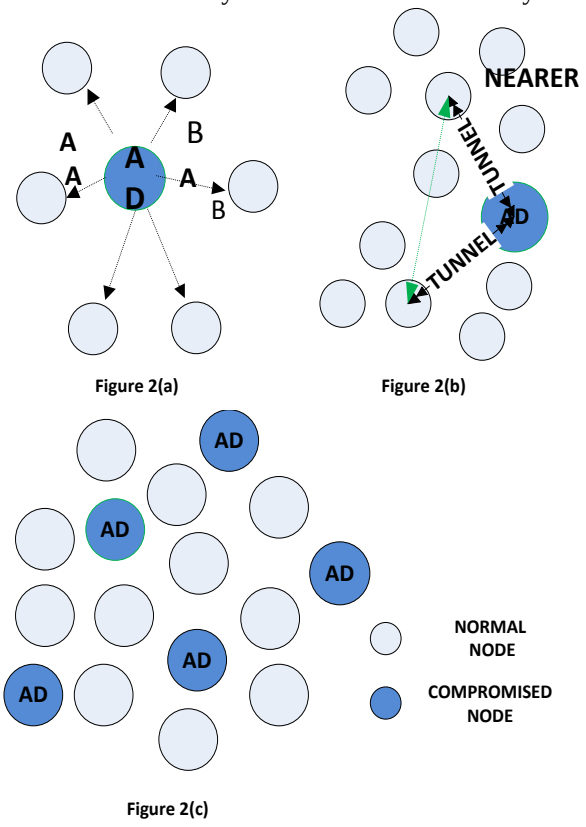


Figure 2

IV. Existing Access Control Protocols In Wireless Sensor Networks

A. Access Control Protocol in Wireless Sensor Networks

Y. Zhou et al. [1] presented Access Control Protocol based on Elliptic Curve Cryptography (ECC) for Wireless Sensor Networks. This access control protocol accomplishes its task of Access Control in WSNs with making generality i.e. node authentication and key establishment for new nodes. Different from conventional authentication methods based on the node

identity, its access control protocol includes both the node identity and the node bootstrapping time into the authentication procedure. Hence this access control protocol cannot only identify the identity of each node but also differentiate between old nodes and new nodes. In addition, each new node can establish shared keys with its neighbors during the node authentication procedure to make secure communication among them. Compared with conventional sensor network security solutions, this access control protocol can defend against most well-recognized attacks in sensor networks like Sybil attack, Eavesdropping, Node compromise attack etc. as well as reduces impact of attack in vicinity of only compromised node and along with achieve better computational and communicational performance.

B. A Novel Access Control Protocol for Secure Sensor Network

H.F.Huang [2] proposed an access control protocol based on Elliptic Curve Cryptography (ECC), on considering the real life implementation of Access Control Protocol in Wireless Sensor Networks of Y. Zhou et al. [1]. It is assumed that Y. Zhou et al.'s Access control protocol is impractical for real life implementation due to insertion of bootstrapping time in authentication and key establishment phase. Huang used cascaded hash chain as a main weapon in authentication and key establishment phase to make this protocol practical. The protocol consists of three phases - an initialization phase, an authentication and key establishment phase and a new node addition phase in its entire life.

INITIALIZATION PHASE: In this phase base station generates secret keys and one way hash function and then preloads it to the nodes. Next base station computes hash chain for each sensor nodes and broadcast these informations to all sensor nodes deployed in sensing region. Also base station publishes materials necessary during authentication and key establishment phase like an Elliptic curve E_q (the elliptic curve E over the finite field F_q), cyclic group with generator P and has an order n etc.

AUTHENTICATION AND KEY ESTABLISHMENT PHASE: In this phase authentication of nodes is performed and along with shared key between pair is also established. This phase executes with handshakes and performs a little bit of computation. This phase also takes a bit of overhead during sharing of parameters. It is here assumed that for each node the broadcasting hash chain will be updated after each successful authentication through the help of base station.

NEW NODE ADDITION PHASE: This phase comes into play when some sensor nodes are lost during network operation. The base station generates secret key and hash function and then load it to newly added node with necessary parameters. And rest of thing is done as old node mentioned above.

C. Enhanced Novel Access Protocol over Wireless Sensor Networks

Hyun et al. proposed an Enhanced Access Control Protocol over WSNs, is a modified version of Huang's proposed protocol [2]. It is shown that Huang's protocol suffers from insecurity towards replay attack and many other active attacks as well as lack of hash chain renewability. Hyun et al. has made NACP more robust and added hash chain renewability. The flaws remained in NACP was due to absence of authentication procedure of Base Station in the new node addition phase and input format of the cascaded hash function. It changes unilateral to mutual authentication process. ENACP also uses a hash chain for the authenticity check of the base station and computed each hash chain by combining a secret key, the same with NACP, along with an additional random value for an initial vector. ENACP is consisted of an initialization phase, an authentication and key establishment phase, and a new node injection phase. At the end of this section, a renewal of hash chain phase is additionally proposed for the hash chain exhausted nodes.

D. A New Design of Access Control in Wireless Sensor Networks

H.F. Huang proposed a simple and efficient Access Control Protocol in WSNs based on ECC and the concept of Schnorr signature [4]. Basically it exploits the concept of time bound in which once time period has elapsed the sensor node in wireless network cannot access any data for future time period. Actually this thing is done in keeping the mind that we have to reduce the impact of long time node compromise problem. Also the proposed scheme presents a simple and efficient authentication and key establishment phase and reduces overhead in a great extent. Like other protocols, the proposed method consists of an initialization phase and an authentication & key establishment phase. During the initialization phase the base station chooses some required parameters used in second phase and feed them into each sensor nodes. Huang also make security aspect for base station and considering public key cryptography for base station. In the case of authentication and key establishment phase, proposed scheme make sure of legitimate sensor node with simple calculation associated keeping time bound criteria. Here a shared key is generated for secure communication among them. It provides more energy and bandwidth saving compare to other proposed schemes. So making much more robust along with offering computational efficiency, bandwidth savings claims a most practical protocol for the resources constrained sensor networks. Its network resiliency makes it more lucrative than others. Thus it is more beneficial in each and every point of views.

E. A New Dynamic Access Control in Wireless Sensor Networks

Hui-Feng Huang et al.'s scheme [7] tries to make most efficient with offering security measure as necessary to exist them in real life implementation. For making its goal, it introduces a very less time consuming and memory consuming operation one way hash function during authentication and key establishment phase of access control

protocol. Also, to make more efficient in communicational overhead, offers a local implementation of mutual authentication and key establishment. It discards the time consuming operation like point multiplication over elliptic curve cryptography. It maintains reduction of consumption of every resources of sensor node as far as possible. It uses a little bit calculational operator like XOR also. So overall it makes each and every effort to make them efficient in each & every angle for resources constrained sensor networks. Its scheme is one of the best but suffers from lack of some security threats.

V. Defensive Measurement Towards Prevailed Security Threats

Access control scheme which are proposed, trying to secure our sensor networks as far as possible. Zhou et al.'s scheme [1] gives the unavailability of private key of CA (certification authority) and prevent from direct deployment of new malicious node in sensor region. No malicious node can eavesdrop the messages in transmission due to availability of pairwise common shared key. Also introducing the bootstrapping time makes wormhole attack, replication attack etc. neutral after expiry of bootstrapping time. So its scheme can withstand with so many attacks. But this access control protocol becomes helpless when adversary attacks at the time of bootstrapping.

H.F. Huang's [2] Novel Access Control Protocol in WSNs made enough security aspects. The proposed protocol is robust against masquerade attack, as adversary can never compute hash chain function in the process of authentication and key establishment with knowing some parameters. So cheating is strictly prohibited in this protocol. Also using random number only one time makes it impossible under replay attack. Again hash chain is updated after each authentication; the attacker cannot use the old hash chain to masquerade legal node. Thus this protocol withstands a forgery attack. But due to unilateral authentication, its security claims comes under peril. Attacker could do the replay attack, just intercepting secrets values broadcasting by base station after the successfully authentication and key establishment phase and after that attacker broadcast a modified secret values except base station and required node. So all nodes consider it as legal values and in near future when that legitimate wants to perform operation through its values but will be rejected from all the other nodes. Using the absence of base station authentication it can easily make new node masquerading attack. Also in this protocol, there is a need of hash chain renewability.

Hyun et al. [3] proposed an Enhanced Novel Access Control Protocol in WSNs which is more robust. Only the legitimate node with valid secret key, valid random number can derive the secret hash chain and thus legal node masquerading attack is not possible under this circumstances. Also There is no way the attacker could know and use the current sessions secret from the hash chain to masquerade as a legal node because each sessions hash value is constantly updated and protected by the onewayness of the hash function. Therefore, ENACP can withstand against the forgery attack. Even if new node masquerading attack is not possible under this scenario. Actually only thing that an attacker should know to masquerade a new legal node is a secret value to derive a correct message with the same as from the legalized base station (or sink node) by using the correct secret value to pass the authenticity check. However, there is no way that the attacker could know the base stations secret value for the correct session due to the onewayness of the hash chain. Along with influence of compromised node in ENACP does not affect to the other node security, thus it could provide more secure connectivity for sensor networks.

H.F. Huang's [4] New Access Control in Wireless Sensor Networks makes a secure network with more energy and bandwidth savings. The proposed method withstands the sensor node replication attack because once the time period elapses, the clones of a compromised node cannot impersonate the real node, also there is no way to know secret values and consequently, without knowing the secret value it is extremely hard to launch node replication attack. In the proposed scheme, the secret key of node is to use the time bounded and the identity for computing signature value (Secret value). Therefore, a compromised node cannot claim a new identity in the vicinity of any other legitimate node and resulting secure against the Sybil attack. Also there is no any possibility to evaluate the secret key of base station and results in no way to change expiration time and identity of node. Further limitation of life time of sensor node also minimizes the impact of node compromise problem. This scheme also makes a secure door against the wormhole attack because tunnel is worked only for life time of sensor node. Thus it prevents wormhole attack after certain time intervals.

Hui-Feng Huang and Kuo-ChingLiu's scheme [7] provides little security with efficient computational and communicational overhead. It provides security against eavesdropping, masquerading attack etc. It mainly focuses upon performances rather than security.
All schemes' security measures are shown in figure 3.

VI. Perfomance of Existing Proposed Schemes

The performances of existing access control schemes are shown in the chart below in terms of computational cost (in terms of the time for computation of one multiplication over elliptic curve, the time for computation of one inverse operation and the time for computation of adopted one way hash function) and communicational overheads. They are shown in chart 1 and 2 respectively.

VII. Conclusion

The Access Control Protocols in WSNs makes a secure gateway in sensor network during new node deployment and access of network's resources. So to make prevention of unauthorized access to WSNs, we resort Access Control schemes in WSNs. This access control schemes maintains authentication to the coming nodes and make a secure communication among the nodes through pairwise secret key developed locally. This survey of access control schemes in

WSNs will give a broad view of readers/researchers how to make access control schemes as well as what should be inserted in the proposed scheme so that it could provide all security measures with little computational cost and less communicational overhead. This will also give a better frame work at a single place. This will also open a research door in the era of secure WSNs i.e. making much more efficient access control mechanism along with perfect network resiliency.

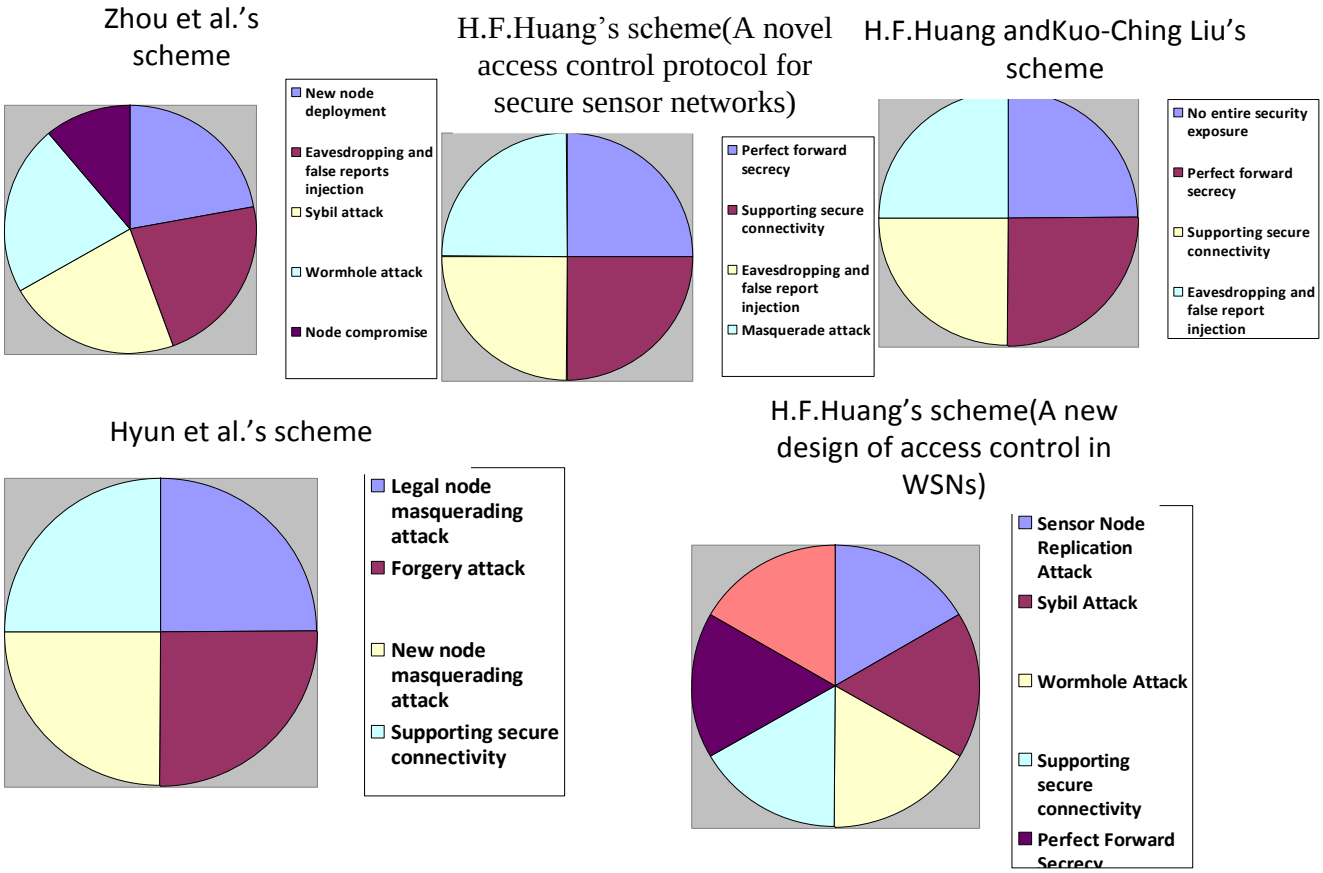


Figure 3.

Chart 1: Computational cost of proposed schemes

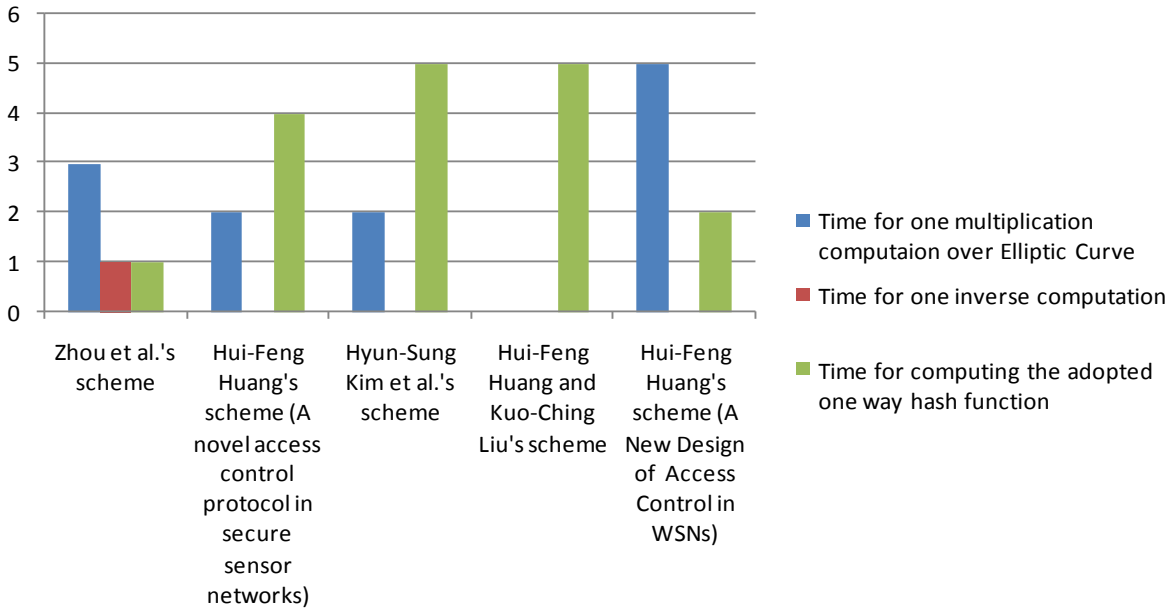
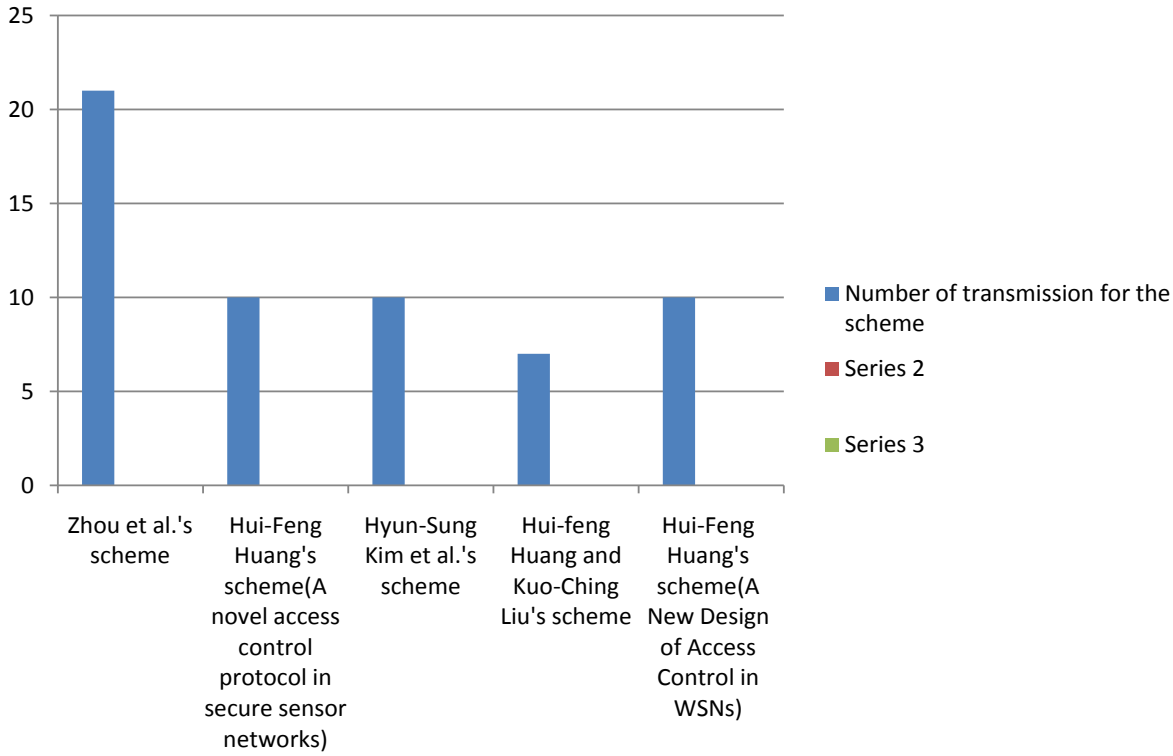


Chart 2: Total number of transmission for the proposed schemes



REFERENCES

[1] Y. Zhou, Y. Zhang, and Y. Fang, "Access control in wireless sensor networks," *Ad Hoc Networks*, vol. 5, pp. 3-13, 2007.
[2] H. F. Huang, "A novel access control protocol for secure sensor networks," Computer Standards & Interfaces, vol. 31, pp. 272-276, 2009.

[3] Hyun-Sung Kim and Sung-Woon Lee, "Enhanced Novel Access Control Protocol over Wireless Sensor Networks," IEEE Transactions on Consumer Electronics, Vol. 55, No. 2, MAY 2009.
[4] Hui-Feng Huang, "A New Design of Access Control in Wireless Sensor Networks," International Journal of Distributed Sensor Networks ,Volume 2011, Article ID 412146, 7 pages.
[5] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, vol. 40, no. 8, pp. 102–114, 2002.
[6] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in Proceedings of IEEE Symposium on Security and Privacy, pp. 197–213, May 2003.
[7] Hui-Feng Huang, Kuo-Ching Liu, "A New Dynamic Access Control in Wireless Sensor Networks," 2008 IEEE Asia-Pacific Services Computing Conference.
[8] N. Koblitz, "Elliptic curve cryptosystems," Mathematics of Computation, vol. 48, pp. 203–209, 1987.
[9] Youssou Faye, Ibrahima Niang, and Thomas Noel, "A Survey of Access Control Schemes in Wireless Sensor Networks," World Academy of Science, Engineering and Technology 59 2011.
[10] W. Diffie and M. E. Hellman, "New directions in cryptology," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, 1976.
[11] Shio Kumar Singh, M P Singh, and D K Singhtise, "A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks," International Journal of Computer Trends and Technology- May to June Issue 2011.
[12] James Newsome, Elaine Shi, Dawn Song, and Adrian Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses," IPSN'04, April 26–27, 2004, Berkeley, California, USA, 2004.
[13] Yih-Chun Hu, Adrian Perrig, and David B. Johnson ,"Wormhole Attacks in Wireless Networks," IEEE journal on selected areas in communications, vol. 24, no. 2, February 2006.
[14] Bo Yu, Bin Xiao," Detecting Selective Forwarding Attacks in Wireless Sensor Networks," 1-4244-0054-6/06/$20.00, 2006 IEEE.
[15] David Martins and Hervé Guyennet, "Wireless Sensor Network Attacks and Security Mechanisms : A Short Survey," 2010 13th International Conference on Network-Based Information Systems.