ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (454-461), Month: April-June 2014, Available at: www.researchpublish.com

A Survey on Sensor Authentication in Dynamic Wireless Sensor Networks

[1]Priya L C, [2]Shantala Devi Patil

[1]M.Tech Scholar, [2]Senior Assistant professor
Department of Computer Science and Engineering
Reva Institute of Technology and Management, Bangalore, India

Abstract: **While applications of Wireless Sensor Network are diversified, several new issues such as mobility of sensor node are raised and bring security issues such as re-authentication and tracing the node movement. In the dynamic sensor network, mobile sensor nodes will continuously move around and frequently reconnect to other sensor nodes. While many security protocols to such networks occur significantly large overheads because their design only considered the static networks. There are several studies on such dynamic environments. In this paper, we show our design for the efficient node authentication and key exchange that reduces the overhead in node re-authentication and also provides untraceablity of mobile nodes. We introduce protocols that are symmetric key crypto system based and public key crypto system based. We also introduce the application scenario of the protocol that is integrated to other networks.**

Keywords: **Neighbour Sink Discovery, Neighbour Sink List (NSL), Node Authentication, Node Reauthentication.**

I. INTRODUCTION

Wireless Sensor Network (WSN) is the network that consists of lightweight devices with short-ranged wireless communication and battery-powered. The devices have the sensor that gathers the environmental information and etc. After sensing this information, the devices send the information to the networks. We define such devices as sensor node, and the core parts of the network as sinks and the base station.

Rapid development of WSNs brought themselves to be deployed to various areas such as RF4CE [19]. However, many security studies on WSNs are rather inefficient to be deployed to such environments. While there are many trials for providing efficient security functions for WSN such as [4, 5, 13, 14], as one of the fundamental security issues, there are various researches on key management in WSN such as key-pre distribution, pair wise key agreement, group key based key agreement, and hierarchical key management schemes. There were also trials of PKI deployment for WSN [17]. In order to reduce the communication overhead from the key establishment, Huang *et al.* [10] proposed public key infrastructure (PKI) based model applying Elliptic Curve Cryptography [15]. However, applying PKI requires larger computational power, although it enables the simplified key agreement procedure.

Since it is obvious that the wireless sensor network will be widely deployed by combining network of static sensor network and mobile entities such as [2, 6], handling a large overhead from frequent node re-authentication requests due to the continuous node movements and the threats of tracing the node movement will be important security issues.
In order to solve such problems, we proposed efficient authentication models that significantly reduce overhead for re-authenticating sensor nodes [7, 8].

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (454-461), Month: April-June 2014, Available at: www.researchpublish.com

II. LITERATURE SURVEY

In this section, we briefly review well-known key agreement protocols designed for the sensor networks. As a commercial solution, Zigbee [3] specifies the key agreement architecture by key predistribution. In their architecture, each node preinstalls its unique keys that are shared with other entities and the network key that is shared with the entire network by the manufacturer. In order to support mobility of a node using a unique key, each node must contain as many keys as the number of nodes. Thus, most studies on authenticated key agreements attempt to increase the efficiency.

2.1 Authenticated Key Agreement Protocols for Static Sensor Networks

Most previous key agreement protocols were based on the symmetric key cryptosystem. Eschenauer and Gligor proposed the pairwise key agreement protocols based on the random key predistribution [5] that enabled the sharing of pairwise keys from the pre-distributed key pool. In their protocol, each node stores *m* number of keys selected from a key pool in the initial stage. After the nodes are deployed, each node shares the key information with its neighboring nodes. When the shared keys are found, the node establishes secure links between the sinks that share the keys. After a link is established, both nodes generate a pairwise key for secure communication. However, the network establishment has a probability of failure that is increased in the case of irregular deployment of sensor nodes or unpredictable interruptions.

Zhu *et al.* [18] introduced the group-key-based key agreement model that minimized threats of compromised nodes. Every node has a unique key, pairwise keys with neighboring nodes, a cluster key shared with all neighboring nodes, and a global key shared with the entire network. However, they assumed that the networks are static.

Abraham and Ramanatha [1] proposed an authentication and initial shared key establishment model in hierarchical clustered networks. Ibriq and Mahgoub [11] proposed an efficient model that deployed a "partial key escrow table" for sinks. Using the key escrow table, a sink can self-generate a shared key for the attached nodes. However, all sinks have to maintain the information of every node in the table to support node mobility.

2.2 Authenticated Key Agreement Protocols For Dynamic WSN

2.2.1 Distributed Authentication Model. Fantacci et al. [8] proposed the distributed node authentication model that does not require the base station to act as the centralized authenticator (CA), as shown in Fig 3. In their model, every node shares partial authentication information of other nodes based on the secret sharing scheme [16]. A node sends an authentication request to another node; e.g., the node N2 is the authenticator and other nodes such as N5 and N6 are distributed authentication servers. The overhead on all nodes in this model is large due to their involvement in the authentication process. Since each node has to participate in the authentication procedures as an authenticator or as an authentication server, the computational and communication overhead would significantly increase as a result of frequent authentication requests. Once a node N1 is authenticated by N2, as shown in Fig 1(a), N1 sends authentication requests to N7, as shown in Fig 1(b). In the figure, N3, N4, N5, and N6 are involved in both authentication processes as authentication servers.

Fig 2: Fantacci's Distributed Node Authentication Model
(a) Initial authentication by 2 *N* (b) 1 *N* reauthenticated by 7 *N*

2.2.2 PKI-based Model. Although PKI brings strong and advanced security services, most studies focused on the symmetric key cryptosystem-based approach, due to the insufficient computational resources for PKI of the sensor nodes. However, many efforts that enable PKI for sensor networks such as Tiny PK [17] and Tiny ECC [15] are often proposed.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (454-461), Month: April-June 2014, Available at: www.researchpublish.com

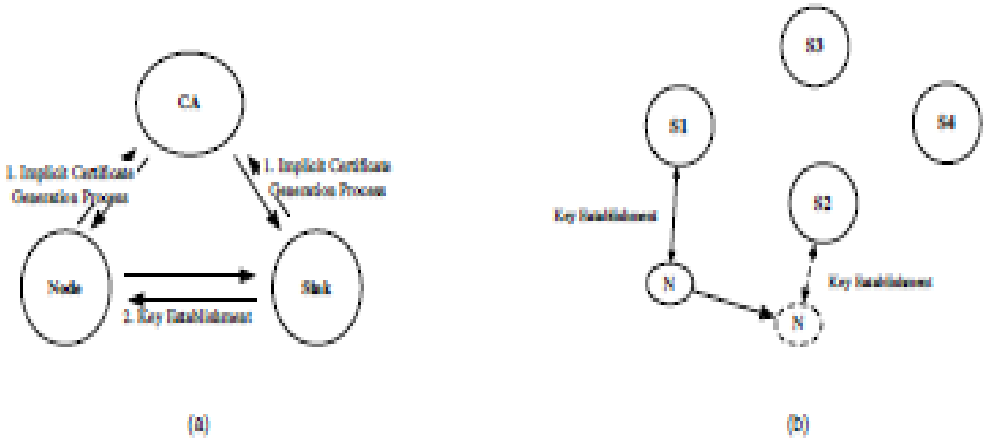

Fig 2: (a) Simplified representation of Huang's Key Agreement Model (b) Applying Huang's model in Dynamic Sensor Network

Huang *et al.* proposed a self-organizing algorithm by using Elliptic Curve Cryptography (ECC) [10]. Huang's model has two phases: *Implicit certificate generation process* and *Hybrid key establishment process*. Once the certificates are issued to nodes, they can self-establish the pairwise keys by exchanging the certificates with other sinks.

Simplified representation of the processes is shown in Fig 2(a). Although Huang *et al.* did not state that their protocol could be applicable to dynamic WSN, their protocol can support node reauthentication. After the certificate is issued to the node *N*, *N* is authenticated by a sink *S1*. When *N* moves and requests the re-authentication to another sink *S2*, *S2* can easily authenticate *N* again as shown in Fig 2(b).

However, their model has two critical problems:

(1) All sensor nodes must contact the CA to obtain their certificates.

(2) Direct contact is required between each sensor node (including mobile sensor node) and the CA, which is not considered practical for large scale networks.

If an implicit certificate is preinstalled to every sink, the advantage of the protocol may be significantly reduced. The other is that every node has to be capable of ECC computation. Even though PKI-based applications for sensor networks will be available in the near future with efficient implementations, the public key-based security architecture still requires more advanced computational power and resources. A sensor node that is only capable of a lightweight cryptosystem such as AES or SHA-1 may not be able to connect to such networks.

III. PROPOSED SYSTEM

While most current security protocols are designed for the static sensor networks and has several problems that applying such models in dynamic environment may occur significantly large resource drain. In this paper, we introduced our efficient model for authenticated key agreement in dynamic WSN and showed several protocols we proposed in [7, 8]. We showed symmetric key based protocol and hybrid protocol that combines symmetric key base model with PKI based model. Our protocols enable the reduced authentication process for the mobile node and can be used in various application of WSN.

In this paper, we show our model that provide high efficiency in such environments and shows several protocols that we previous introduced in [7,8].

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (454-461), Month: April-June 2014, Available at: www.researchpublish.com

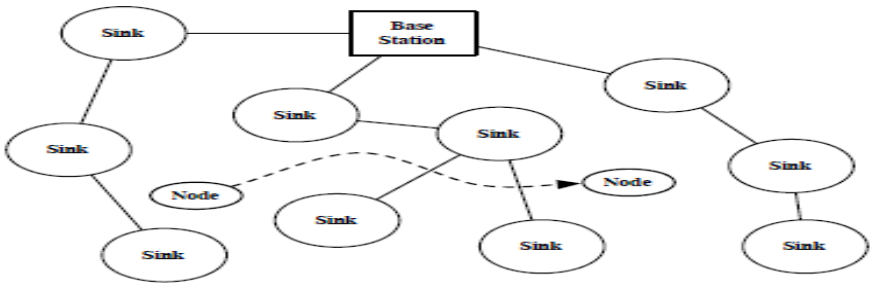

Fig. 3

Fig 3: A dynamic mobile node continuously moves in the sensor networks that static sinks established. The unbroken line denotes the static connection between sinks and the base station. The dotted line denotes the movement of the mobile node.

In this section, we claim the security issues on the node mobility in WSN and problems of previous authentication and key agreement models. In pa [kyusuk1, kyusuk2, kyusuk3], we defined a sensor network model with moving nodes as in Fig 3. We also defined a static sensor node as Sink, a mobile node as Node, and the base station that is the core network. The node has linear movements in the network. The base station and sinks are static as same as Ibriq and Mahgoub's model [11]. Sinks act as the gateway that link nodes to the base station, and the base station is a kind of headquarter that manages entire networks. When a node initially joins the network, the node connects to a sink in the network and is authenticated by the sink with help of the base station. After that the node moves and reconnects to other sink. In the model, the sink that reauthenticates the node is the neighbor sink of the sink that previously authenticated the node. The reauthentication processes frequently happen due to the node continuously moves in the network.

In practical scenarios, re-authentication happens when a node lost connection to the sink or moved and connected to other sink. For the former case, the node can be easily re-authenticated to the same sink when the connection becomes available again. For the latter case, the node request the re-authentication to other sink that is the near to the previously attached sink.

For such environments several security Issues raise as followings.

3.1 Frequent Re-authentication. Since the sensor have low powered battery and low-end processor with short-range wireless communication, the reducing communication and computational overheads is important to increasing the lifetime of the sensor. However, the mobile sensor node may occur the large overhead for the security computation due to the frequent requests of node reauthentication. When a node connects to a sink, the sink has to authenticate the node. When the node connects to other sink after the movement, the new sink has to authenticate the node again. If the node has continuous movement, the authentication process will also occur repeatedly. It is obvious that the frequent re-authentication processes are the significant factors that drain the resources in battery based sensor nodes.

However, the current authentication and key distribution protocols are insufficient to be applied in such environment with lack of consideration of the node mobility. Using the current protocols such as [11, 1], the communication overhead for reauthentication is as same as previous authentication.

Such overhead will be the problem in the environment that the frequent movements of the large number of nodes are happened. Thus, the less computational and communication overheads in reauthentication are very urgent requirement for the node mobility support in the WSN.

3.2 Tracing Node Movements. Considering the mobility of sensor nodes, the tracking of the node movement is one of possible attacks. When the mobile nodes are deployed in battlefields, the tracking by enemies is significant threats for the networks. Thus, the authentication and key agreement protocols should not reveal the node movement.

IV. IMPLEMENTATION

Our proposed system is implemented as three modules they are Base station, Sink and Sensor Nodes.
Base Station: This act as the Main Central Authority (CA), where it helps in registering the sinks like it will generate the keys particularly and loads in its database. While registering it will ask for the port number of an sink as shown in the Fig.4.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (454-461), Month: April-June 2014, Available at: www.researchpublish.com

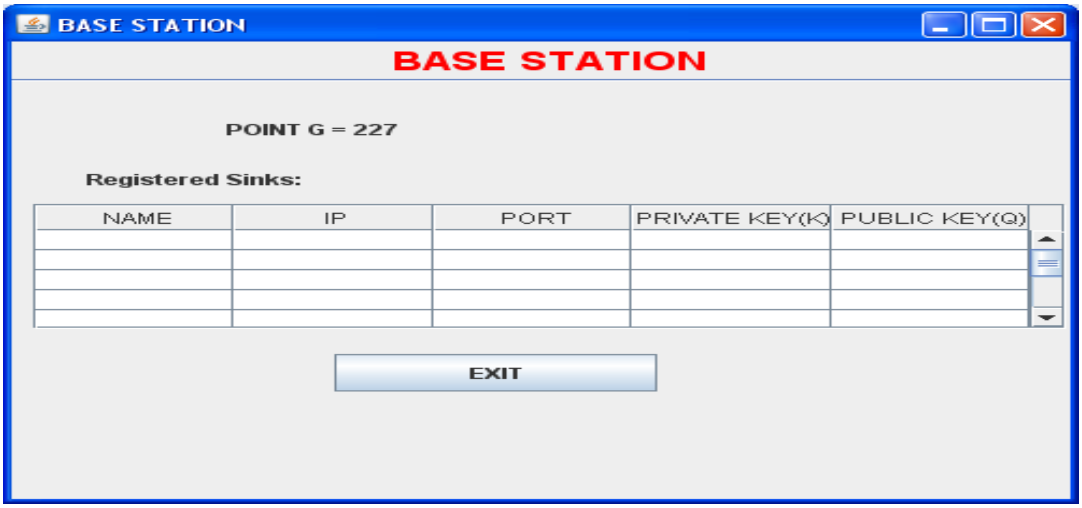

Fig 4: Base Station

Sink: After the creation of the sink, it will check for the neighbor sink. If any sink is found, then it will exchanges the keys and request is processed as shown in Figures.

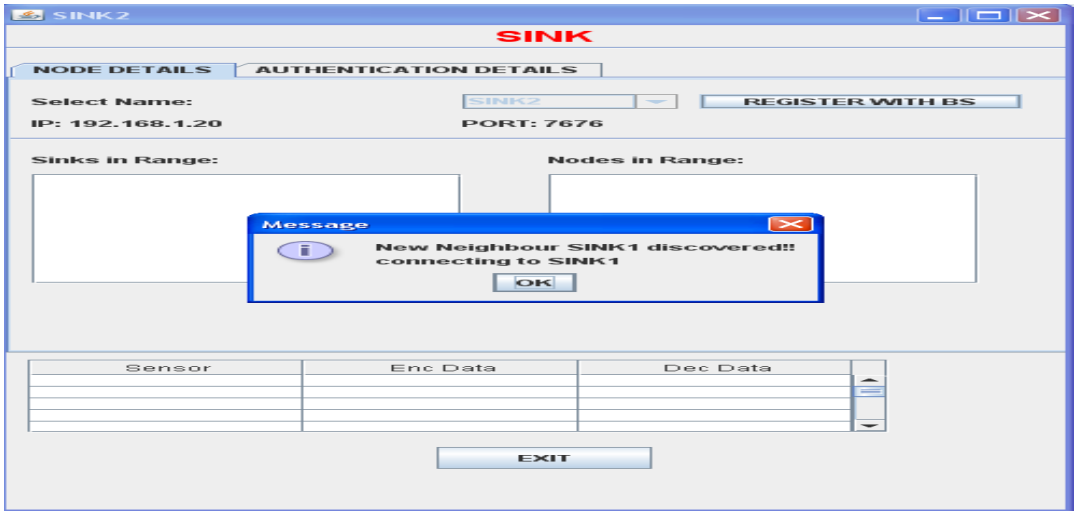

Fig 5: Neighbor discovery

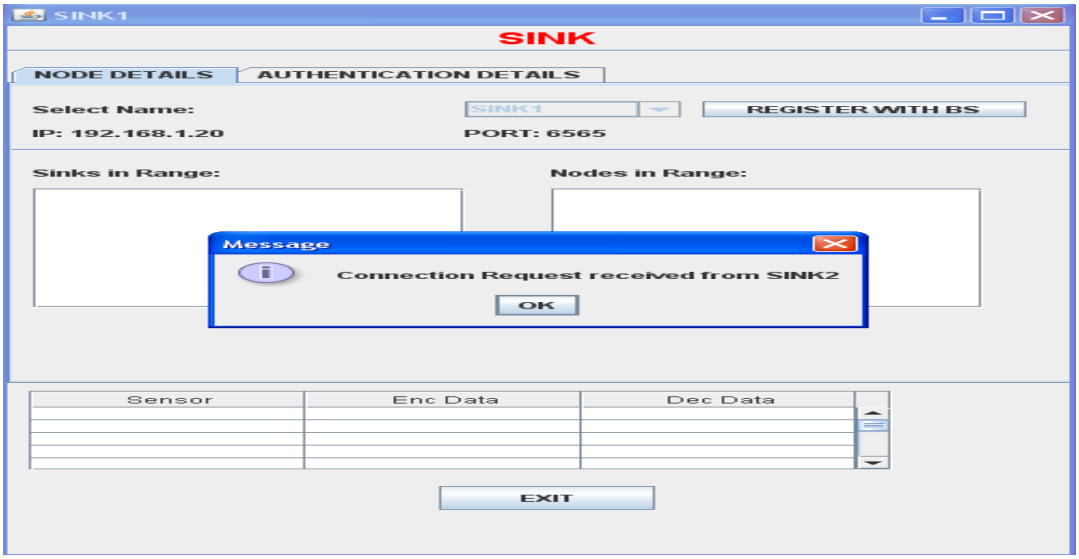

Fig 6: Requesting for the connection

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (454-461), Month: April-June 2014, Available at: www.researchpublish.com

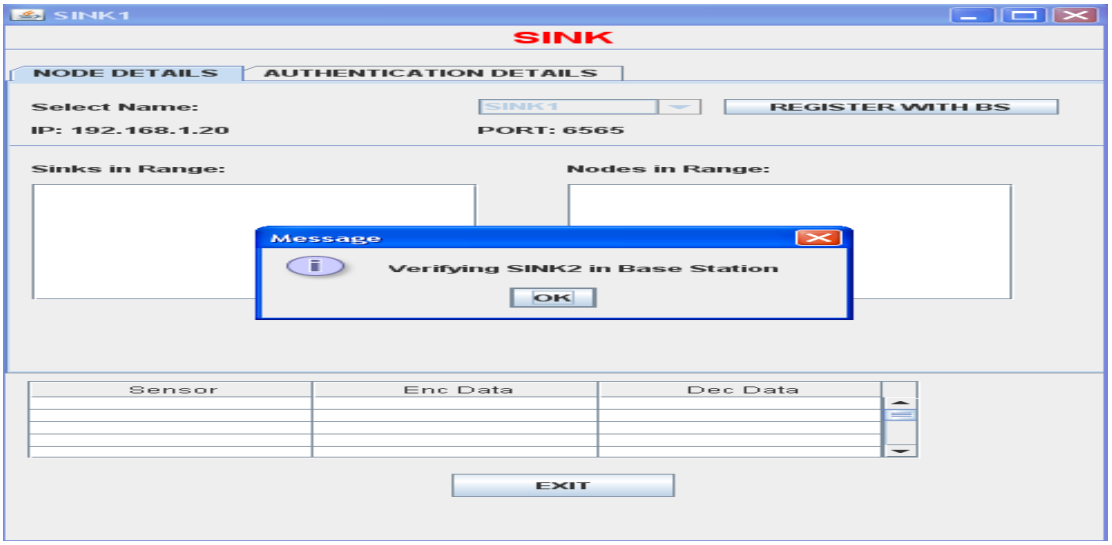

Fig 7: Verifying Sink in BaseStation

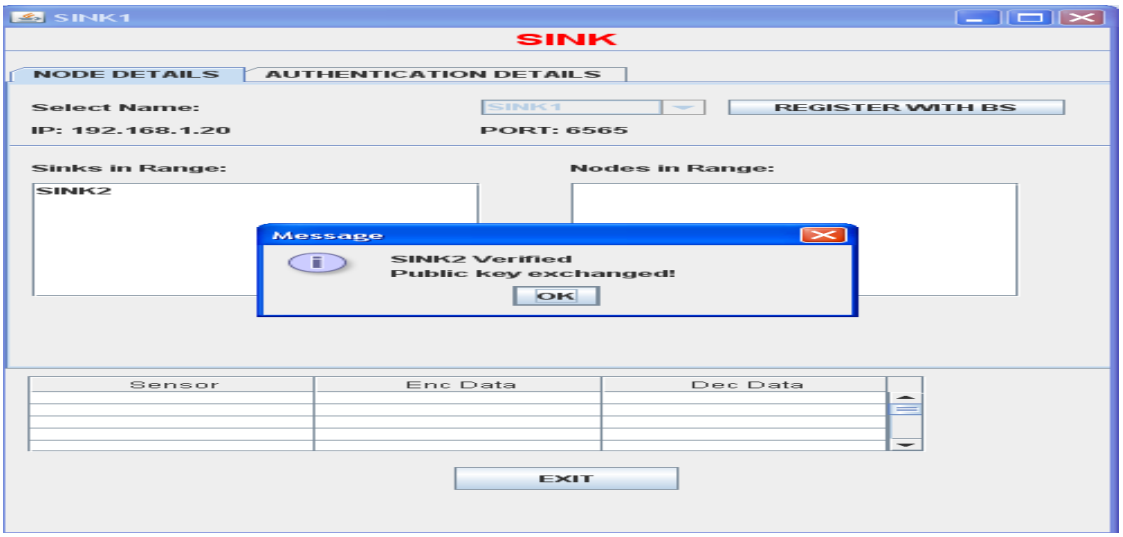

Fig 8: Keys Exchange between the sinks

Sensor Node: When the sensor node is created, it has to be registered to the sink which is in the range of it(Fig 9).

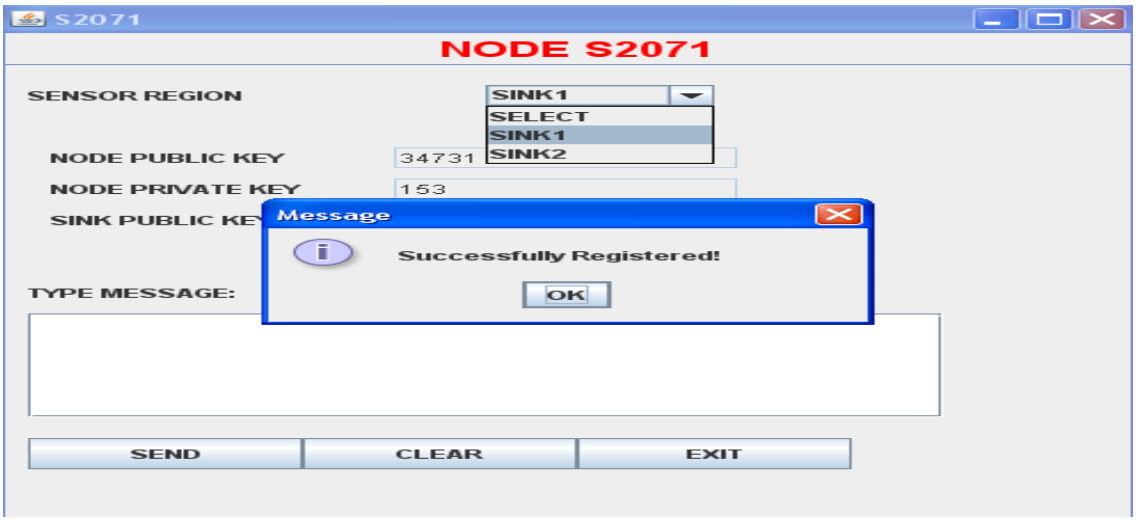

Fig 9: Registration of the Sensor Node

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (454-461), Month: April-June 2014, Available at: www.researchpublish.com

After registration, the node can sent the message to the sink(Fig 10)

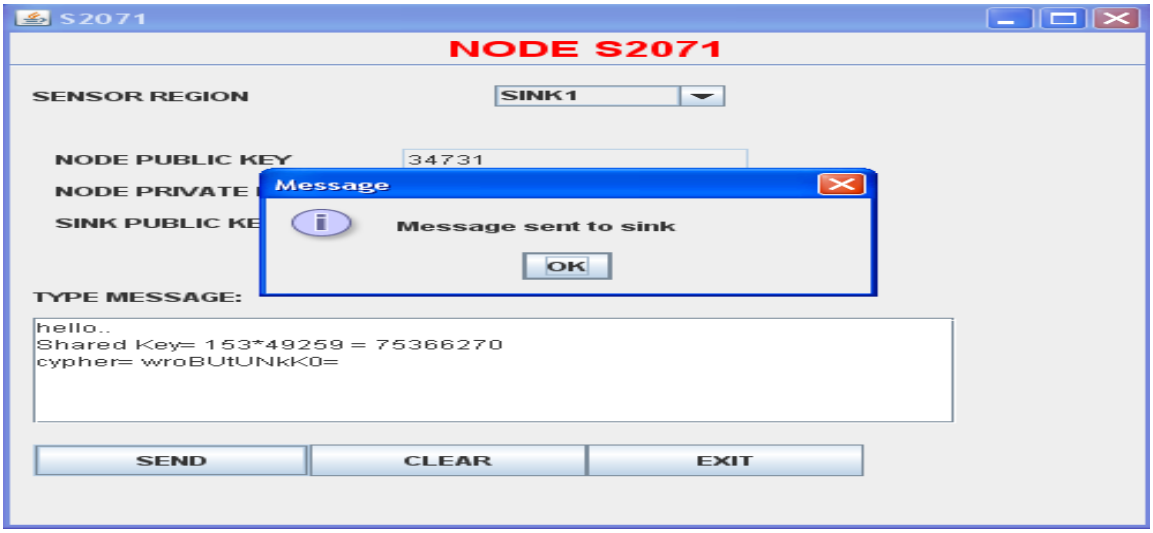

Fig 10: Node Sending Message to the Sink

While the same is decrypt in the sink using the keys respectively(Fig 11)

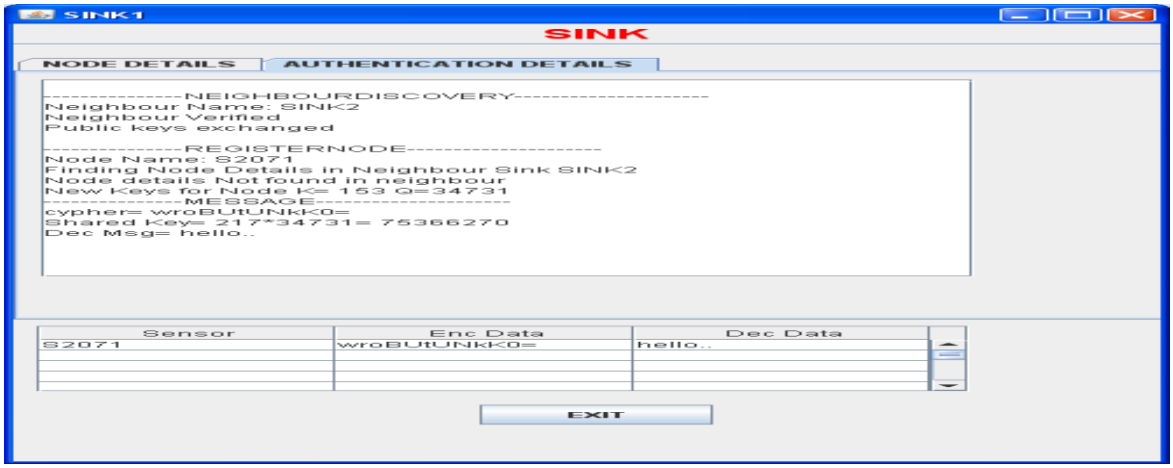

Fig 11: Sensor Node Details in the Sink

V. CONCLUSION

While most current security protocols are designed for the static sensor networks and has several problems that applying such models in dynamic environment may occur significantly large resource drain.

In this paper, we introduced our efficient model for authenticated key agreement in dynamic WSN and showed several protocols we proposed in [7, 8]. We showed symmetric key based protocol and hybrid protocol that combines symmetric key base model with PKI based model.

Our protocols enable the reduced authentication process for the mobile node and can be used in various application of WSN.

REFERENCES

[1] Jibi Abraham and K S Ramanatha. An Efficient Protocol for Authentication and Initial Shared Key Establishment in Clustered Wireless Sensor Networks. Proceeding of Third IFIP/IEEE International Conference on Wireless and Optical Communications Networks, 2006.

[2] Ian F. Akyildiz and Ismail H. Kasimoglu. Wireless sensor and actor networks: research challenges. Ad Hoc Networks, 2(4):351 - 367, 2004.

[3] William C Craig. Zigbee: Wireless Control That Simply Works. Zigbee Alliance, 2005.

[4] Jeremy Elson and Deborah Estrin. Random, Ephemeral Transaction Identifiers in Dynamic Sensor Networks. 21st International Conference on Distributed Computing Systems, :pp. 0459, 2001.

[5] L. Eschenauer and V.D. Gligor. A key management scheme for distributed sensor networks". In Proceedings of the 9th ACM conference on Computer and Communications Security (CCS). Washington. DC. USA, :41-47, 2002.

[6] Gill, K. and Shuang-Hua Yang and Fang Yao and Xin Lu. A Zigbee-based home automation system. IEEE Transactions on Consumer Electronics, 55(2):422-430, 2009.

[7] Kyusuk Han and Kwangjo Kim and Taeshik Shon. Untraceable Mobile Node Authentication in WSN. Sensors, 10(5):4410-4429, 2010.

[8] Kyusuk Han and Taeshik Shon and Kwangjo Kim. Efficient Mobile Sensor Authentication In Smart Home and WPAN. IEEE Trans. on Consumer Electronics, 56(2):591-596, 2010.

[9] Kyusuk Han, Kwangjo Kim, Wook Choi, Hyohyun Choi, Jungtaek Seo, Taeshik Shon, Efficient Authenticated Key Agreement Protocols for Dynamic Wireless Sensor Networks, Ad Hoc & Sensor Wireless Networks, Volume 12 , Number 3 , Mar 2012, pp , ISSN: 1551-9899

[10] Qiang Huang and Johnas Cukier and Hisashi Kobayashi and Bede Liu and Jinyun Zhang. Fast authenticated key establishment protocols for selforganizing sensor networks. WSNA '03: Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications, 2003.

[11] J. Ibriq and I. Mahgoub. A Hierarchical Key Establishment Scheme for Wireless Sensor Networks. Proceedings of 21st International Conference on Advanced Networking and applications (AINA'07), :210-219, 2007.

[12] C. Karlof and D. Wagner. Secure routing in wireless sensor networks. In Proc. of SNPA'03, Anchorage, Alaska, :113-127, 2003.

[13] Chris Karlof and Naveen Sastry and David Wagner. TinySec: a link layer security architecture for wireless sensor networks. SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems, 2004.

[14] HangRok Lee and YongJe Choi and HoWon Kim. Implementation of TinyHash based on Hash Algorithm for Sensor Network. Proceedings of World Academy of Science, Engineering and Technology, 10:135-139, 2005.

[15] An Liu and Peng Ning. TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks. 2008 International Conference on Information Processing in Sensor Networks, 2008.

[16] Adi Shamir. How to share a secret. Communications of the ACM, 22(11):612--613, 1979.

[17] Ronald Watro and Derrick Kong and Sue-fen Cuti and Charles Gardiner and Charles Lynn and Peter Kruus. TinyPK: Securing sensor networks with public key technology. Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, :59-64, 2004.

[18] Zhu, Sencun and Setia, Sanjeev and Jajodia, Sushil. LEAP+: Efficient security mechanisms for largescale distributed sensor networks. ACM Trans. Sen. Netw., 2(4):500--528, 2006.

[19] ZigBee alliance. RF4CE Standard Specification Release 1.0. 2009.