[Proceeding] An Authentication and Key Establishment Scheme for the IP-Based Wireless Sensor Networks

Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Computer Science 10 (2012) 1039 – 1045

Procedia Computer Science

The 7th International Symposium on Intelligent Systems Techniques for Ad hoc and Wireless Sensor Networks (IST-AWSN)

An Authentication and Key Establishment Scheme for the IP-Based Wireless Sensor Networks

Sarmad Ullah Khan[a], Claudio Pastrone[b], Luciano Lavagno[a], Maurizio A. Spirito[b]

[a]*Electronics Department, Politecnico di Torino, Turin, Italy*
[b]*Pervasive Technologies Research Area, Istituto Superiore Mario Boella (ISMB), Turin, Italy*
Email: {sarmad.khan, luciano.lavagno}@polito.it, {pastrone, spirito}@ismb.it

Abstract

Integration between wireless sensor networks and traditional IP networks using the IPv6 and 6LoWPAN standards is a very active research and application area. A combination of hybrid network significantly increases the complexity of addressing connectivity and fault tolerance problems in a highly heterogeneous environment, including for example different packet sizes in different networks. In such challenging conditions, securing the communication between nodes with very diverse computational, memory and energy storage resources is at the same time an essential requirement and a very complex issue. In this paper we present an efficient and secure mutual authentication and key establishment protocol based on Elliptic Curve Cryptography (ECC) by which different classes of nodes, with very different capabilities, can authenticate each other and establish a secret key for secure communication. The analysis of the proposed scheme shows that it provides good network connectivity and resilience against some well known attacks.

Keywords: Authentication; Security; Key establishment; 6LoWPAN; Elliptic Curve Cryptography;

1. Introduction

Recent research activities in the field of LoWPANs aim to integrate sensors and actuators into traditional IP networks using IPv6 over LoWPAN (6LoWPAN)[9] . Smart objects belonging to a 6LoWPAN can directly communicate with an IPv6 host, thus allowing data processing operations to be performed in standard servers. 6LoWPAN actually enables the integration of smart objects into the overall Internet, toward the definition of the Internet of Things (IoT). In such resulting scenario, the presence of billions of objects raises additional issues in terms of scalability, manageability, addressing, security, privacy, secure mobility and robustness. Therefore an efficient redesign of the Internet architecture and the definition of new protocols are required to cope with the above challenges in the future Internet. In fact, several projects from industrial and international collaboration are being carried out to define the future internet architecture which would solve the limitations of the current architecture [11] including security, mobility and interoperability for the heterogeneity of networks.

In this context, mobility support for the small and smart devices is one of the main important issues since it is utilized for realizing many innovative applications. Mobile communication may increase fault tolerance capabilities of a network but it requires continuous connectivity among the nodes in the network and with the clusters and could also introduce new threats against the privacy, integrity and confidentiality. Here, we specifically focus on authentication and on securing the communication between the nodes in the real deployment of 6LoWPANs.

The main contribution of this paper is to provide a robust authentication and key establishment technique while maintaining better network connectivity compared to the key pre-distribution schemes and resilience against some well

1877-0509 © 2012 Published by Elsevier Ltd.
doi:10.1016/j.procs.2012.06.144

known attacks. The paper is organized as follows: Section 2 introduces the related work, while the proposed solution is discussed in Section 3. Section 4 describes the possible attacks and their counter measures in the proposed scheme. Finally, Section 5 concludes the paper.

2. Related Work

A number of cryptographic mechanisms have been introduced in the literature for secure authentication and encryption in WSNs such as block ciphers as part of standards-based protocols, including IEEE 802.15.4, different variants of symmetric and asymmetric cryptography. While these mechanisms are optimized to suite the resource constrained sensor and actuator networks, in case of 6LoWPAN networks, where the networks are integrated into the internet, such cryptographic mechanisms can still experience poor performance due to the size of the packets exchanged and the length of the keys. Furthermore, it is difficult to distribute the security keys in the federated combination of networks. Thus these mechanisms need to be modified to suite the resulting IoT scenario.
Hsiu in [1] proposed a mutual authentication scheme for wireless sensor networks based on the elliptic curve cryptography while Huang in [2] proposed fast key generation algorithm for the ECC based cryptography by optimizing the scalar multiplication which consume nearly 80% of the time needed for the total key calculation. This optimization is done by proposing the 1's complement subtraction to represent scalars in scalar multiplication which offers less hamming weight and improve the efficiency of scalar multiplication. Qing in [3] presented a mutual authentication scheme for wireless sensor networks based on the elliptic curve cryptography to reduce the computational cost in the authentication phase by using a fast multiplication algorithm. Arazi in [4], [5] presented the group key generation technique based on the ECC for the clustered based wireless sensor networks. They presented a novel algebraic approach for partitioning the key generation process. They distributed the computational load among neighboring nodes to decrease the execution time and balancing the power consumption. Holohan in [6] proposed an authentication scheme using virtual certification authorities. Each virtual authority is assigned randomly some certificates signed by different certification authorities. Each node contact this virtual authority to verify the certificate of other nodes but this scheme produces a large overhead in the case if virtual certification authority doesn't have a valid certificate of a node and he needs to contact other virtual certification authorities.
Reza in [7] presented a symmetric key establishing protocol for the heterogeneous wireless sensor networks using the public/private key. In this approach, every node is assigned its public/private key pair and a symmetric key. The gateway node is also assigned the public keys of all the nodes in the networks and its own public/private key pair. Each node sends its pubic key to the gateway. The gateway then compares the received public key with the stored one for the authentication purpose. This scheme cannot provide the security against the man-in-the-middle attacks and Denial-of-Service (DoS) attacks. Also it has a large communication overhead during the authentication phase. Khan in [12], [13] presented an authentication and key establishment schemes for the heterogeneous wireless sensor networks to reduce the communication overhead and memory cost. Their OMNET++ simulation results show that these schemes provide good network connectivity and resilience against node capture attack while keeping the energy cost at low level compare to the existing key pre-distribution schemes for the homogeneous and heterogeneous wireless sensor networks. Raza in [8] represented a secure End-to-End (E2E) communication protocol between the IP enabled sensor networks and the traditional internet using the compressed and light weight design implementation of IPSec. Their performance evaluation in terms of code size, packet overhead, and communication performance shows that their proposed scheme has a comparable overhead to the generally deployed 802.15.4 link layer security while it offers a true E2E security. Jara in [9],[10] proposed a secure mobility management scheme for the 6LoWPAN based on the ID/Locator split architecture and on the extension of the Return Routability with Diffie-Hellman key agreement and ECC. Their proposed solutions deal efficiently with the DoS attacks and flooding attacks against the ID/location update messages, home registration and binding transfer process. They verified and evaluated the schemes successfully with the AVISPA tool.

3. Proposed Scheme

Here we describe the proposed authentication and key establishment phases for IP-enabled wireless sensor and actuator networks based on 6LoWPAN. Since the total number of hosts in a network could vary a lot and and the

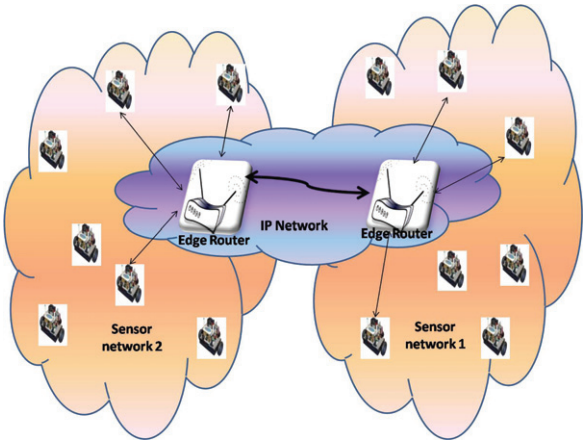

Figure 1: Virtual Network Architecture

network might also contain thousands of nodes, the use of key pre-distribution techniques could not represent the most proper solution. In fact, such mechanisms require large memory space that could be not available in resource constrained smart objects. In addition, the nodes are expected to move and may leave their current network and enter into a foreign network. Therefore, we introduce a new approach based on the Elliptic Curve Cryptography (ECC) that supports a higher security level compared to the standard encryption techniques (RSA, AES), while using shorter key length and introducing less computational overhead. In this approach, the joining network easily authenticates the incoming node by generating its authentication key instead of getting the nodes authentication key from nodes previous network in order to reduce the total communication overhead during the authentication of the incoming mobile node, also avoiding the introduction of new vulnerabilities.
The reference network model considers two sub networks connected with each other through edge routers as shown in fig. 1. In addition, a specific node in the network acts a reference for the different supported security functionalities and it is called Network Security Manager.

3.1. Offline Key Assignment

Important key materials are assigned offline to each node and are used to authenticate each other by generating the authentication key and to secure the communication link by generating a public/private key pair for encryption and decryption of the messages. More specifically:

- To each entity of the network a random number is assigned by the Network Security Manager after a node registration phase
- To each entity of the network one share of the public key is also assigned, while the other share of the public key would be generated by the relevant local Network Security Manager
- When considering the secure communication between two nodes in the network, source IP and destination IP are used to generate a specific elliptic curve (adopted just for the pair of nodes taken into account)
- Each entity and a network has its own generator G_e and G_n respectively

3.2. Authentication

Authentication is an important and initial step in the network security that allows a trusted node to access the network resources and establishes secure links with other nodes of the network while it prevents an adversary to gain access to those resources and exploit possible vulnerabilities. Here, we describe how two nodes belonging to different networks can authenticate with each other.
Due to large number of entities (smart objects and IP hosts) in the network, it would not be a feasible solution to provide an authentication key(s) to an entity especially when it belongs to a resource constrained network (i.e. sensor

network). In fact, (1) nodes usually have limited memory space and cannot store a large number of keys for secure communication with a very large number of entities of all networks (2) nodes are inherently prone to security attacks e.g., sensor nodes can easily be captured and their stored keys reused (3) partial distribution of keys reduces the network connectivity in the considered federated large networks. Hence we use an online key generation approach based on the ECC to reduce the memory consumption and avoid the key revocation/renewal in case of node capturing attack.

Every node is provided with a prime number 'p' that would be used to generate the private key for a particular destination node. It is worth stressing that each node would have one public key for all the destination nodes belonging to different networks. This public key consists of two shares (1) node share and (2) network share. The purpose of the network share is just to confirm that the node belongs to the mentioned network. The destination node needs to generate the public key of a source node by getting those shares from the source node and from the Network Security Manager of the source node as

$$PublicKey = f\{Node\ Share,\ \ Network\ Share\} \tag{1}$$

For example, a Sensor Node (SN_1) of one network wants to establish a communication link with a sensor node (SN_2) of other network. During the registration phase of a SN with its Network Security Manager, it sends the *node share* of its public key to its Network Security Manager. The Network Security Manager generates the *network share* of the registering SN public key and also sends the *network share* along with a random number to the SN. When a SN_1 wants to communicate with the SN_2, it asks its Network Security Manager to get the random number and *network share* of SN_2 from the SN_2 Network Security Manager which is assigned by the SN_2 Network Security Manager to the SN_2 during the registration phase. The SN_1 Network Security Manager gets that random number and *network share* from SN_2 Network Security Manager using its secure link, already established, and also sends the random number of the SN_1 and the *network share* of the SN_1 public key. The SN_1 creates a private key for the SN_2 after getting that random number and sends its own generated public key share to the SN_2 in the joining request signed by its private key. When the SN_2 receive this message, it contacts it local Network Security Manager for the *network share* of the public key and a random number of the SN_1. The SN_2 Network Security Manager forwards the *network share* of SN_1 public key and its random number to the SN_2 which it receives during the random number exchange. Once the SN_2 receives the *network share*, it generates the public key of the SN_1 and authenticates the message signature. The *node share* and the *network share* are generated as follow

$$NodeShare = S = IP_{Network} \,.\, c \,.\, G_{SN} \mod P_{SN} \tag{2}$$

$$NetworkShare = T = S \,.\, G_N \mod P_N \tag{3}$$

$$PublicKey = Node\ Share \ \oplus \ Network\ Share \mod P \tag{4}$$

Where (P_{SN}, G_{SN}) and (P_N, G_N) are the pair of prime number and group generator of the network entity and the Network Security Manager respectively, c is the point on elliptic curve and 'P' is the prime field generator.

After successful authentication, SN_2 accept the join request of the SN_1 and generate a private key for that SN_1 using the same procedure and sends its own share of public key to the SN_1 signed by its private key. The SN_1 generates the public key of the SN_2 by getting the *network share* from the SN_2 Network Security Manager through its own Network Security Manager and verifies the signature. In this way, both SN_1 and SN_2 authenticates each other.

3.3. Private Key Generation

Since every node generates and uses a separate private key for authentication and secure communication with the nodes of other networks for its public key, here, we describe the procedure of generating a private key. Since all nodes of every network are registered with their Network Security Manager , the Network Security Manager assigns a unique random number to each registered member. That number is used to generate a private key by other nodes to communicate with that particular node of that network. After the generation of public key by the destination node, it performs the XOR of the public key with the provided random number. The source node also gets that number from the Network Security Manager of the destination node through its own Network Security Manager. The source node uses that number to generate the private for the destination node.

$$Private\ Key = (Public\ Key \ \oplus \ Random\ Number)^{-1} \mod P_{SN} \tag{5}$$

3.4. Handover

Since SNs are mobile, they may leave one network and enter into another one. To avoid node replication and Sybil attacks, it is necessary to update the node's public key and private key. To do so, the public key and the private key should be a function of some network parameters and also do not introduce a large communication overhead in case of fast mobility. In addition, the public key of the mobile node should be updated in such a way that there is no interruption in the ongoing communication. Finally, the private key should be updated accordingly.
Here we describe the proposed approach for updating the keys by considering a simple scenario that can implement the suggested idea easily without introducing communication overhead. Assume that a sensor node SN_1 belongs to its parent network X and after some time it moves to network Y. It sends its *node share* to the Network Security Manager of the network Y. Its public key in network X is

$$PublicKey_X = S \ + \ T_X \ \ mod \ \ P \tag{6}$$

When SN_1 moves to network Y, then its public key will be

$$PublicKey_Y = S \ + \ T_Y \ \ mod \ \ P \tag{7}$$

According to the suggested approach, to avoid any interruption in the ongoing communication,

$$PublicKey_X \ = \ PublicKey_Y \ \ \Rightarrow \ \ S \ + \ T_X \ = \ S \ + \ T_Y \ \ mod \ \ P \tag{8}$$

Since the Network Security Manager Y receives the *node share* of the joining node SN_1, it generates the *network share* T_Y and sends back to the joining node.

$$T_Y \ = \ S \ . \ G_Y \ \ mod \ \ P_Y \tag{9}$$

Since, T_Y is different from T_X because of different network generators, the node will generate a number 'd' such that it makes the T_Y equals to T_X as

$$d \ . \ T_X = T_Y \ \ mod \ \ P_{SN} \ \ \Rightarrow \ \ d \ = \ T_Y \ . \ T_X^{-1} \ \ mod \ \ P_{SN} \tag{10}$$

The generated 'd' is sent to the destination node encrypted with its previous private key: in this way, the destination node can update the public key of the source node. After that, the source node also updates its private key.

4. Performance Evaluation

In order to evaluate the proposed scheme in terms of total time consumed during the exchange of key establishment packets, we used cooja simulator [14]. The simulation environment consists of two sub networks as shown in fig.1 and we vary the total number of nodes in each sub network. Initially, each sub network consists of 4 nodes and then we increased them to 8, 12 and 20. More specifically, we consider four sensor nodes in one network aiming to establish a secure key with the four nodes of the other sensor network by varying the total number of nodes in each network. The results shown in fig. 2(a) describe the total time consumed during the first key establishment process with the node of other network while fig. 2(b) shows the simulation environment of cooja.
Here, we describe some well known attacks that could be possible in the IP based wireless sensor networks and show that how the proposed scheme deals with those attacks.

4.1. Connectivity

Connectivity is the fundamental aspect and plays an important role in the network performance. However, it suffers due to the security protocols implementation in terms of partial key distribution and management, especially in a resource constrained wireless sensor networks where the connectivity depends on the key matching probability and hence there is always a trade off between the memory, connectivity and computational cost. Since, the proposed scheme is based on the ECC in which each node has public/Private key pair for secure communication and also in the proposed scheme, if a node wants to establish a communication link with other nodes of the network, it just generates the public key of those nodes their public key shares from the Network Security Managers and there is no need for anything to be common among the nodes. So, the connectivity of the network in the proposed scheme is always 100% compared to the key pre-distribution schemes in which the connectivity is based on the common shared keys.

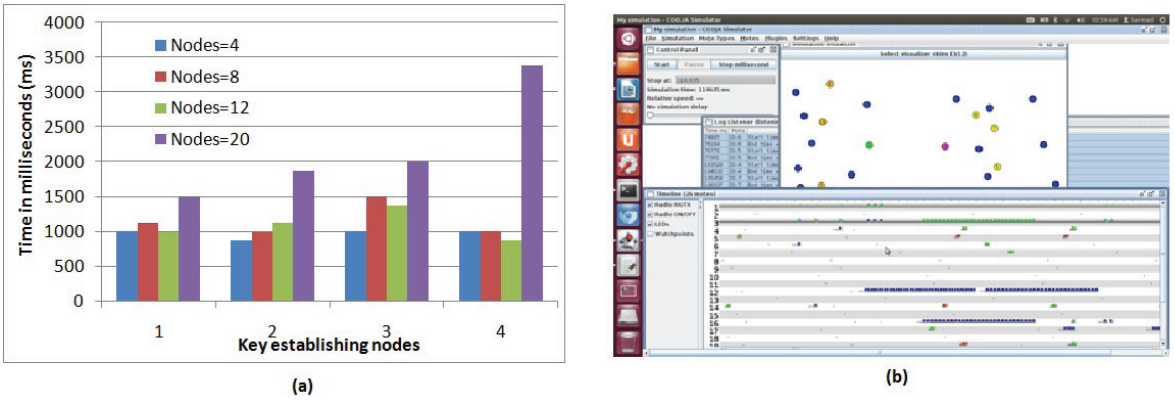

Figure 2: (a). Time taken by a node during the exchange of key establishment messages in ms (b). Network topology in Cooja

4.2. *Sniffing*

During the exchange of the pubic key materials (i.e. the node share and the network share), an adversary might capture those packets to get those shares. But, obtaining those shares does not allow the adversary to construct the node's public key because the construction of public key also requires the destination node random number assigned by its Network Security Manager during the registration phase. Thus an adversary cannot get that random number until the destination node gets compromised by the adversary. Since the nodes are mobile, their public key and the private key is also updated when they change the network (because of the network share of the public key). Hence the packets sniffing do not help the adversary to construct the node public key and exhaust its resources by sending some fake packets.

4.3. *Stolen ID Attack*

An adversary might steal the IDs of the authentic member of the network and capture the node share of the public key of that node and can pretend itself as an authentic node. In the proposed scheme, if the destination node receives the link establishment requests (containing the node share of the public key) from an adversary whose ID is the authentic node ID, the destination node generates the public key of the received authentic node ID by getting its random number from Network Security Manager but that key would not be able to verify the message signature because authentic node private key would not be compatible with the private key of the adversary node. In order to establish the link with the destination node, an adversary is also required to steal the private key of that authentic node as well. Also the adversary node would not be able to generate the public key of the victim node because it cannot get the required random number of the victim node and the network share from the Network Security Manager which is used in the public key generation. And hence will be detected quickly in the network.

4.4. *Denial of Service Attack*

Denial of Service (DoS) attack is the one in which an adversary tries to isolate a node from a network and keeps it busy to exhaust its resources by sending some useless data. In the proposed solution, this is only possible if the adversary, somehow, gets an access to the network and become its authentic member or by stealing the nodes IDs and their shares of public key. The adversary would use those IDs and shares in establishing a link with the destination node of the other network. But this would not work because the adversary would need to sign that message again after updating its time stamp and by doing so, the destination node would not be able to verify that message with the generated public key. This helps the destination node to identify any malicious activity and inform its Network Security Manager which will inform the Network Security Manager of source node about those fake messages.

4.5. *Node Replication Attack*

Sensor nodes are very vulnerable and can be easily captured, analyze and replicate by the adversary in various positions in the network. Such attacks may allow the adversary to corrupt data and may disconnect significant parts

of the network.
Since all the nodes in the sensor networks are mobile and their positions changes frequently depending on their speed and the size of network, their position should be updated by their Network Security Managers immediately in case of leaving or joining the network. Thus the adversary cannot replicate the nodes of one network into another network.

5. Conclusion

In this paper, an authentication and mutual key establishment scheme is proposed for IP based wireless sensor network (6LoWPAN). This scheme has good theoretical results against some well known attacks and also take less time to exchange the key establishment packets. The proposed solution is analyzed theoretically as well as using cooja for time estimation but in future, the work we will be analyzed using cooja for the total energy consumption, overhead during the handover and connectivity.

6. Acknowledgments

This work has been supported by “COMPLEX–COdesing and power Management in PLatform-based design space EXploration (247999)” and “BUTLER–uBiquitous, secUre inTernet-of-things with Location and contExt-awaReness (grant no. 287901)” projects, funded by the European Commission under FP7.

References

[1] Hsiu L. Y.; Tien H. C.; Pin C. L.;Tai H. K.; Hsin W. W.;, A Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography , International open access journal on the science and technology of sensors and biosensors, pp. 4767-4779, ISSN 1424-8220, May 2, 2011.
[2] Xu Huang, Pritam Shah, and Dharmendra Sharma, Fast Algorithm in ECC for Wireless Sensor Network, IMECS 2010, Hong Kong, 2010.
[3] Qing Chang; Yong-ping Zhang; Lin-lin Qin; , ”A node authentication protocol based on ECC in WSN,” Computer Design and Applications (ICCDA), 2010 International Conference on , vol.2, no., pp.V2-606-V2-609, 25-27 June 2010.
[4] Arazi, O.; Qi, H.; , ”Self-certified group key generation for ad hoc clusters in wireless sensor networks,” Computer Communications and Networks, 2005. ICCCN 2005. Proceedings. 14th International Conference on , vol., no., pp. 359- 364, 17-19 Oct. 2005.
[5] Arazi, O.; Elhanany, I.; Rose, D.; Qi, H.; Arazi, B.; , ”Self-certified public key generation on the intel mote 2 sensor network platform,” Wireless Mesh Networks, 2006. WiMesh 2006. 2nd IEEE Workshop on , vol., no., pp.118-120, 25-28 Sept. 2006.
[6] Holohan, E.; Schukat, M.; , ”Authentication Using Virtual Certificate Authorities: A New Security Paradigm for Wireless Sensor Networks,” Network Computing and Applications (NCA), 2010 9th IEEE International Symposium on , vol., no., pp.92-99, 15-17 July 2010.
[7] Reza Azarderskhsh; Arash Reyhani-Masoleh;, Secure Clustering and Symmetric Key Establishment in Heterogeneous Wireless Sensor Networks, EURASIP Journal on Wireless Communications and Networking, Article ID 893592, Hindawi Publishing Corporation, October 2, 2010.
[8] Raza, S.; Duquennoy, S.; Chung, T.; Yazar, D.; Voigt, T.; Roedig, U.; , ”Securing communication in 6LoWPAN with compressed IPsec,” Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011 International Conference on , vol., no., pp.1-8, 27-29 June 2011.
[9] Jara, A.J.; Marin, L.; Skarmeta, A.F.G.; Singh, D.; Bakul, G.; Daeyeoul Kim; , ”Secure Mobility Management Scheme for 6LoWPAN ID/Locator Split Architecture,” Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2011 Fifth International Conference on , vol., no., pp.310-315, June 30 2011-July 2 2011.
[10] Jara, A.J.; Marin, L.; Skarmeta, A.F.G.; Singh, D.; Bakul, G.; Daeyeoul Kim; , ”Mobility Modeling and Security Validation of a Mobility Management Scheme Based on ECC for IP-based Wireless Sensor Networks (6LoWPAN),” Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2011 Fifth International Conference on , vol., no., pp.491-496, June 30 2011-July 2 2011.
[11] Papadimitriou, D.; Tschofenig, H.; Rosas, A.; Zahariadis, S.; et al; Fundamental Limitations of Current Internet and the path to Future Internet, European Commission, FIArch Group, Ver. 1.9, 2010.
[12] Khan, S.U.; Lavagno, L.; Pastrone, C.; Spirito, M.; , ”An effective key management scheme for mobile heterogeneous sensor networks,” Information Society (i-Society), 2011 International Conference on , vol., no., pp.98-103, 27-29 June 2011
[13] Khan, S.U.; Pastrone, C.; Lavagno, L.; Spirito, M.A.; , ”An energy and memory-efficient key management scheme for mobile heterogeneous sensor networks,” Risk and Security of Internet and Systems (CRiSIS), 2011 6th International Conference on , vol., no., pp.1-8, 26-28 Sept. 2011.
[14] Joakim, E.; Fredrik, .; Niclas, F.; Nicolas, T.; Adam, D.; Thiemo, V.; Robert S.; Pedro, J.M.; ”COOJA/MSPSim: Interoperability Testing for Wireless Sensor Networks” SIMUTools 2009, Rome, Italy.