An Energy and Memory-Efficient Key Management Scheme for Mobile Heterogeneous Sensor Networks

An Energy and Memory-Efficient Key Management Scheme for Mobile Heterogeneous Sensor Networks

Sarmad Ullah Khan[1], Claudio Pastrone[2], Luciano Lavagno[1], Maurizio A. Spirito[2]
[1]Electronics Department, Politecnico di Torino, Turin, Italy
E-mail: {Sarmad.Khan, Luciano.Lavagno}@polito.it
[2]Pervasive Technologies Research Area, Istituto Superiore Mario Boella (ISMB), Turin, Italy
E-mail: {pastrone, spirito}@ismb.it

Abstract— **Wireless Sensor Network (WSN) technology is being increasingly adopted in a wide variety of applications ranging from home/building and industrial automation to more safety critical applications including e-health or infrastructure monitoring. Considering mobility in the above application scenarios actually introduces additional technological challenges, especially with respect to security. The resource constrained devices should be robust to diverse security attacks and communicate securely while they are moving in the considered environment. To this aim, proper authentication and key management schemes supporting node mobility should be used. This paper presents an effective mutual authentication and key establishment scheme for heterogeneous sensor networks consisting of numerous mobile sensor nodes and only a few more powerful fixed sensor nodes. Moreover, OMNET++ simulations are used to provide a comprehensive performance evaluation of the proposed scheme. The obtained results show that the proposed solution assures better network connectivity, consumes less memory, has low communication overhead during the authentication and key establishment phase and has better network resilience against mobile nodes attacks compared with existing approaches for authentication and key establishment.**

Keywords—Heterogeneous Sensor Networks; Mobile Nodes; Fixed Nodes; Security;

I. INTRODUCTION

Wireless Sensor Networks (WSNs) consist of a number of constrained devices with limited resources in terms of computational power, communication capability and memory/storage resources. Such nodes are usually characterized by low cost, low power and multifunctional capabilities making them suitable for ubiquitous and pervasive applications such as home/building, industry automation, environmental monitoring, health-care and even military surveillance. WSNs can be deployed in both controlled (e.g., buildings) and uncontrolled locations (e.g., public spaces).

The inherent WSN characteristics including resources scarcity, limited communication bandwidth and ad-hoc networking capability introduce many challenges also with respect to secure communication. To assure a certain level of security, specific countermeasures need to be selected in order to protect the nodes from diverse possible attacks. However, the limited resources hinder the adoption of classical security approaches. As a consequence, new security solutions suitable for WSNs are being defined. More specifically, key management can be considered as the basic foundation upon which other security primitives are built. Researchers have proposed a number of key management schemes in the literature. Asymmetric cryptography (RSA) and the Elliptic Curve Cryptography (ECC) were initially considered not to be suitable for most sensor applications due to their high computational cost, energy consumption and storage requirements. Nevertheless, recent studies showed that public key cryptography such as Elliptic Curve (due to small key size and low computational overhead) and Rabin's scheme (due to fast encryption/decryption time compared to RSA) might be feasible even in sensor networks [7][8].

WSNs can be basically divided into two main categories (1) homogeneous sensor networks and (2) heterogeneous sensor networks. Homogeneous sensor networks attracted most of the researcher's attentions in developing the security algorithms. However, their fundamental scalability and performance limitations [9, 3], proved by both theoretical [2] and simulation analysis [3], forced researchers to think about Heterogeneous Sensor Networks (HSNs) incorporating a mixture of nodes with widely varying capabilities [4]. Yarvis [11] increases average delivery rate and network life time without increasing the cost by introducing energy and link heterogeneity along with the proper deployment of HSNs. Duarte-Melo and Liu analyzed energy consumption and life time of HSNs in [6] by providing periodic data from the sensing field to remote receiver.

This paper proposes an online key generation and management scheme for HSNs, extending the work presented in [32]. *The main contribution of this paper is to reduce the communication overhead and energy consumption by optimizing the initial node authentication step*, which is fundamental to keep the energy cost of the overall approach low. This paper also *introduces a novel mutual authentication and key establishment procedure maintaining better network connectivity and resilience against node capture attacks compared to competing approaches*. The paper is organized as follows: Section 2 introduces the related work; Section 3 describes the proposed scheme, while OMNET++ simulation results are discussed in Section 4. Finally, Section 5 concludes the paper.

II. RELATED WORK

This section provides an overview of state of the art key management schemes that have been presented in literature for both homogeneous and heterogeneous WSNs.

Perrig et al. [16] presented SPINS, a centralized keying method for sensor networks in which each node contains a secret key whose corresponding key is stored in the base

station and uses one-way hash chains for creating an epoch-delayed key release mechanism for the use in authenticated broadcast. However, two sensor nodes cannot have a common secret key directly. If two nodes A and B want to establish a communication key with each other, A sends a request to B, which creates and forwards a token to the base station. The base station then generates a session key for A and B, encrypts it with the secret keys that it shares with A and B and then sends encrypted data to A and B respectively. Since the nodes use the base station as a trusted server to establish a secret key, this scheme will not work if the base station is not reachable or has a high communication overhead, especially in the case of multi-hop communication.

Eschenauer and Gligor [12] proposed a random key pre-distribution scheme that does not require the base station for the key establishment between any two nodes. According to this scheme, a set of randomly selected keys from a large pool is assigned to each sensor node before the network deployment. Two nodes communicate directly to establish a secret communication key only if they have at least one key in common. Chan [13] further improved the security of [12] by introducing the "q keys" concept. To establish a secret key, two nodes must share at least q keys but this scheme requires storing a large number of keys in each sensor node. Liu [7] presented a key establishment scheme using a prior knowledge of node deployment coupled with Rabin's scheme [1] to achieve a high degree of connectivity (while reducing the memory cost) and network resilience against the node capture attacks. Zhang [22] presented the NPKPS pairwise key pre-distribution scheme for WSNs to achieve better security, connectivity and efficiency and less memory cost compared to [12]. Efficient authentication schemes are proposed in [30] and [31] which improve over past work in terms of security, authentication overhead and storage requirements.

In order to present a key management scheme that reduces energy cost and supports node mobility, Kim [23] proposed a level-based key management scheme for multicast communication that has reasonable routing overhead and low mobility management overhead. For mobility supported cluster-based WSNs, a two-layered dynamic key management scheme was proposed by Chuang [24] while polynomial-based key pre-distribution scheme for mobile sensor networks was proposed by Blundo [14]. Sarmad [32] presented a runtime key generation scheme for the authentication and secret key establishment to reduce the memory cost and increase the network resilience. Camtepe and Yener [15] proposed a combinatorial design approach for key pre-distribution. First they proposed a simple key pre-distribution scheme based on Finite Projective Plane (FPP) which provides direct key establishment, tolerance to node capture and no computational and communication overhead, but with limited network scalability and resilience and without node authentication. Their hybrid approach augments scalability of the initial scheme to the cost of sacrificing direct connectivity.

Sanchez and Baldus [18] apply an FPP design to the pre-distribution of Blundo polynomial shares. Their approach enables direct pairwise key establishment for a large number of nodes independent of the physical connectivity of the WSN. To reduce the memory overhead and support node mobility among different networks, Maerien [27] proposed the MAnagement of Secret keYs protocol (MASY) for mobile WSNs which assigns to a node only one symmetric key, shared only with the back-end server of its network, and which assumes a trust relationship between the newly entered network and the node's old parent network.

For HSNs, Du [17] presented an unbalanced key pre-distribution scheme to improve network connectivity, reduce memory overhead and provide better network resilience compared with existing key management schemes for homogeneous sensor networks. Nodes with high capabilities are assigned m keys, while nodes with low capabilities are assigned l keys, $m>>l$. Sarmad [26] presented a two key pool approach for secret key generation in mobile HSNs which reduces the memory overhead and increases network resilience compared to [17]. Zhang [29] presented a group oriented key management scheme for HSNs in which a large key pool is split into a sub key pool for each group, while a routing-driven key management scheme based ECC is presented by Du [8]. Their results show better connectivity and network resilience than [12], [17]. Symmetric key distribution based on public key cryptography using prior knowledge of sensor deployment location provides better resilience against node capture, as well as lower memory cost and computational overhead [20]. Sajid [19] presented an online generation of secret key by storing a small number of generation key in each sensor node before the deployment of HSNs. Two low capability nodes request a high capability node to discover a shared generation key between them and use a random number to generate a secret communication key. In order to support node addition and node revocation, Poornima [21] proposed a tree based key management scheme for HSNs while Xinyu Jin [28] presented an Unpredictable Software-based Attestation Solution (USAS) for compromised node detection in mobile sensor networks.

III. PROPOSED SCHEME

In this section, the proposed key establishment scheme for HSNs is presented. The reference network model defines a HSN composed of a Base Station (BS), Fixed Nodes (FNs) and Mobile Nodes (MNs). These nodes are heterogeneous in terms of computational power, memory and energy resources. However, the same communication technology is adopted. The BS and the FNs are powerful devices while MNs are characterized by very limited resources and can change their position within the given environment following a specific mobility model. Moreover, the MNs are more numerous than the FNs, and only the FNs need to be equipped with tamper-resistant hardware.

In this resulting scenario, the BS only communicates with the FNs and acts as a trusted server for them. To address scalability issues, a cluster-based approach has been adopted (similarly as in [32]). In fact, FNs act as Cluster Heads (CHs) and are in charge of managing authentication and key establishment operations for a group of MNs.

A. *Proposed Scheme Overview*

Node authentication and key establishment are the basic security features provided by the proposed solution. First the authentication phase is performed among the FNs and the MNs. Once the authentication phase is successfully completed, key establishment operations can be performed among the MNs and FNs. The proposed scheme supports mobility by providing the two considered functionalities in a scenario where MNs move from one cluster to another one. Fig. 1 depicts the main operations of the proposed scheme for the HSNs.

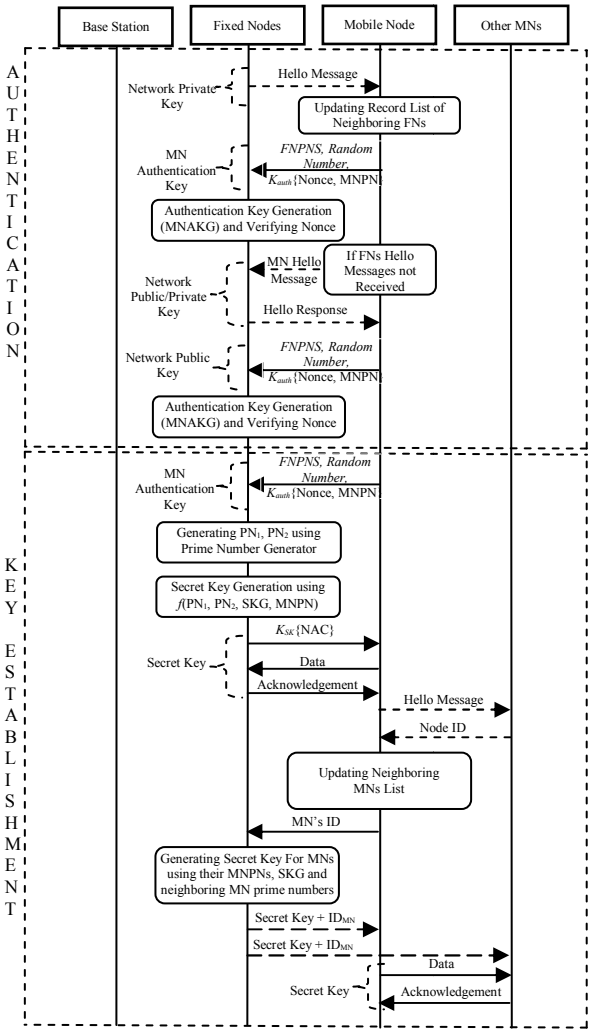

Figure 1. Overview of proposed algorithm

B. *Key Pre-Distribution*

In this section, key pre-distribution among the FNs and the MNs is described. A secret key (SK) is assigned to every MN; more specifically, such key is generated using a Secret Key Generator (SKG), a prime number that is pre-assigned to each MN of the network (MNPN), and the two randomly generated prime numbers (using MNPN and SKG as a seed to the prime number generator) using a one way secret key generation function *f( )*. The key establishment procedure is discussed in section *III.E*.

Each FN is provided with the following key material: the public key of the BS, its own public/private key pair, a one-way authentication key generation function *g(),* a Secret Key Generator (SKG) and a one way secret key generation function *f( ),* a Compromised Node Detection Key (CNDK) and a network private key (K_{prt}) along with its own prime. It is worth noting that FNs must also implement a fast key revocation algorithm [25] in order to protect the Secret Key Generator (SKG) and the network private key.

As far as the MNs are concerned, the following key material is considered: a secret key (SK), a network public key K_{plc}, an authentication key K_{auth}, the Fixed Node Prime Number Sum (FNPNS), its own prime number and a random number.

C. *Cluster Formation*

Once the network is deployed, FNs start the cluster formation phase. During the cluster formation phase, all the FNs periodically broadcast a Hello messages to neighboring MNs for a given number of times (3-times in the proposed scheme). Such messages include nodes IDs and a random nonce encrypted using the *network private key*. It is assumed that the FNs are deployed such that most MNs receive Hello messages from more than one FN. The selection of FN as a CH depends on the Hello message signal strength. Each MN also keeps a list of neighboring FNs from which it has received Hello messages to possibly identify backup CHs. If, for some reason, the MNs do not receive any FN Hello message within a given time period, they start broadcasting Hello message including a nonce encrypted by the *network public key* to discover authentic neighboring FNs. Fig. 2 describes the virtual network organization.

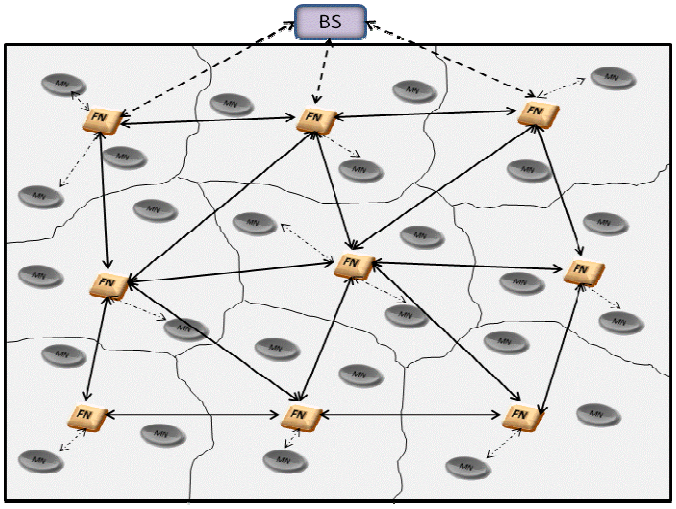

Figure 2. Network topology

1. FN → * : Hello, H(K_{prt}{Hello})
2. MN → * : Hello (if FN Hello is not received)
3. FN → MN : Hello-Resp., H(K_{prt}{Hello-Resp.})

D. *Mobile Nodes Authentication*

To get access to the network, each MN needs to authenticate itself with a selected CH. To do so, the MN sends a "Join request" encrypted using the *network public key*. The request includes the *Fixed Node Prime Number Sum*, a

random number related to its authentication key and the nonce provided within the Hello Message sent by the selected CH along with its own prime number encrypted by MN's authentication key. Once received such information, the CH is able to infer the authentication key of the MN by using one-way authentication key generation function *g()* as follows

$$K_{auth} = g(FNPNS, random\ number, SKG) \quad (1)$$

Successful decryption of the encrypted nonce and *MN prime number* by the CH using the inferred K_{auth} proves the MN authenticity. It is worth noting that the use of SKG in K_{auth} generation guarantees that an authentic FN is actually generating the K_{auth} and that *MN prime number* is not revealed to any adversary node. After the authenticity check, the FN sends the joining confirmation and a Network Authentication Code (NAC) to the MN. This is used to reduce the authentication burden while the MN moves through different clusters within the same network. The *Network Authentication Code* is also periodically updated as a countermeasure to replay attacks or node replication attacks performed by an adversary.

1. MN → CH : FNPNS, Random Number, K_{aut}{Nonce, MNPN}
2. FN : Generate K_{auth} using MNAKG and Verify Nonce
3. CH → MN : NAC

E. Key Establishment and Management

To secure communication between the CH and the MN, each MN is assigned a secret key SK while its generation function is assigned to the FNs before the deployment. During the authentication phase, each CH receives the *MN prime number*s of its member MNs. CHs using these *MN prime number*s and the *secret key generator* SKG generate the first prime number using prime number generator (PN_1); this prime number is further combined with the *MN prime number*s and *secret key generator* SKG to generate the second prime number (PN_2). Then, the CH generates the required *secret key* using a *one way secret key generation function f( ),* thus obtaining the same secret key owned by the specific MN

$$Secret\ key = f(PN_1, PN_2, MNPN, SKG) \quad (2)$$

For secure communication between the MNs, a secret key between them is generated by the CH. For instance, if a mobile node A wants to establish a direct communication link with mobile node B, it sends its ID_A along with the ID_B to its CH. Then the CH generates a *secret key* for them using their IDs, *prime numbers* and *one way secret key generation function f( )* and sends it to both MNs using the *secret key* shared with each of them. CHs also periodically inform the BS about their member MNs to avoid the node replication attacks in the network.

1. MN → CH: FNPNS, Random Number, K_{aut}{Nonce, MNPN}
2. CH : Generate PN_1, PN_2 and *SK*
3. CH → MN: *SK*{Join ACK, NAC}

F. Mobile Nodes Leaving and Joining Clusters

During the movement of a MN to perform its task, it may move from one cluster to another cluster in the network. To provide full connectivity to MNs, FNs are deployed such that each MN should normally receive Hello messages from more than one FN. One of the FNs is selected as a CH by the MN based on the Hello message received signal strength, while information about other neighboring FNs is kept as a backup. A MN moves from one cluster to another cluster if it finds its CH signal strength dropped below a certain threshold during its periodic check. Before the transition to the new cluster, a MN sends broadcast Hello messages to discover new neighbors and update the relevant list. Once the CH is selected base on the signal strength of the Hello message response, the MN sends to the old CH a leaving message also including the new CH ID and sends a join request containing the *Network Authentication Code* to the new CH. After the verification of the *Network Authentication Code*, the new CH contacts the old CH of the MN asking for its *prime number*. If the old CH received the leaving message from its MN including the new CH ID, it confirms the MN movement to the new CH by sending the *MN prime number* and also informs the BS to avoid node replication attacks. After receiving the *MN prime number*, the new CH accepts the joining request from the incoming MN. If, due to e.g., poor radio coverage or packet losses, the MN leaving message is not received by its previous CH and its joining request is received by the new CH, then upon the reception of the *MN prime number* request from the new CH about its MN, the previous CH tries to contact its MN to confirm the transition. If it receives a positive response from its MN or no response, it sends the *MN prime number* to the new CH and also informs the BS that the specific MN is moving to another CH. After receiving the *MN prime number*, the new CH generates the *secret key SK* of this MN and informs the BS about new MN ID. The old CH deletes this MN from its MN members list and the BS updates the MN members lists related to the other CHs in order to avoid node replication attacks.

1. MN → * : Hello
2. FN → MN : Hello-Resp., H(K_{prt}{Hello-Resp.})
3. MN : Verify Hello using K_{plc} and select new CH
4. MN → new CH : K_{plc}{NAC}
5. MN → old CH : New CH ID
6. new CH → old CH, BS : MNPN request using the FN public key
7. old CH → new CH : MNPN using the FN public key

G. Addition of New Mobile Nodes

MNs are unreliable devices with limited power supply; hence they may fail or run out of power over time. This can cause coverage and connectivity problems in WSNs, significantly degrade network performance and shorten network lifetime. To overcome these problems, some MNs could be replaced and new MNs would be added in the network. However, adding new MNs poses new challenges for security schemes such as the establishment of security keys with the existing FNs and MNs; in fact, newly deployed MNs could be compromised or could be malicious nodes.

In the proposed scheme, a newly deployed MN is pre-loaded with a special authentication code along with the authentication key. The BS is in charge of informing the FNs about the addition of the new MN, also providing the relevant ID and a special authentication code. The purpose of this

special authentication code is to avoid the Sybil attacks in which an adversary can create multiple copies of the compromised MN with new IDs and introduce them as new nodes in the network.

The newly added MN broadcasts a Hello message encrypted using the network public key to discover its neighboring authentic FNs. This Hello message includes the MN ID and special authentication code. Upon the reception of Hello message from the new MN, neighboring FNs will check the special authentication code by comparing it with the BS-provided code. After successful verification, FNs send their cluster identities and authentication nonce encrypted using the *network private key*. After receiving the response from the neighboring FNs, the MN will select one of the authentic FNs having the best signal to noise ratio as its CH and will send a joining request to establish a secret key and get the *Network Authentication Code* from its CH.

IV. Analysis and Evaluation

In this section, the proposed scheme is analyzed using the OMNET++ simulator, in terms of network connectivity, network resilience against node capture attacks, energy consumption, memory cost and communication overhead. The simulation results have been obtained using OMNET++ 4.1 with the mobility framework MiXiM 2.0.1. The simulation scenario is defined by a network composed of 500 MNs and 16 FNs. The size of the network simulation area is 400m x 400m. Both the FNs and the MNs use the 802.15.4 CSMA and radio specification based on the CC2420 radio chip. The transmission power is set to 10mW and sensitivity is set to -95dBm for all nodes. The mobility of the MNs is described by the random walk mobility model in which the speed of the MNs is constant but a random direction is chosen periodically within a predefined range. More specifically, the speed of the MNs is set to 1m/s and their direction update interval to 0.1s. The simulations were repeated 3 times for 5000 seconds for each result.

Result comparison of the proposed solution with other existing key management protocols shows better network connectivity and resilience, with a significant reduction in memory and communication overhead.

A. Network Connectivity

In order to show the effectiveness of the proposed solution in terms of network connectivity, the simulation results of the proposed scheme are compared with [12], [17], [26] and [29] where the connectivity depends on the key sharing probability. For a balanced key pre-distribution scheme, the single key sharing probability between the MN and the FN is given by

$$Pr[Conn] = 1 - \frac{(P-K)!\,(P-K)!}{P!\,(P-2K)!} \qquad (3)$$

where K is the number of keys assigned to FNs and MNs from a pool of P keys. Instead, for the unbalanced key pre-distribution [17, 26] scheme, the single key sharing probability is given by

$$Pr[Conn] = 1 - \frac{(P-K)!\,(P-S)!}{P!\,(P-S-K)!} \qquad (4)$$

where K is the size of the key pool assigned to each MN and S (S>>K) is the size of the key pool assigned to each FN.

In the proposed scheme, the K_{plc} is assigned to each MN and the K_{prt} to each FN before network deployment. These two keys connect a MN to an authentic FN of the network. Hence the connectivity of the network is almost 100% if and only if the FN is not compromised. Fig. 3 shows the comparison of OMNET++ simulation results for the network connectivity of the proposed scheme with [12], [17], [26] and [29].

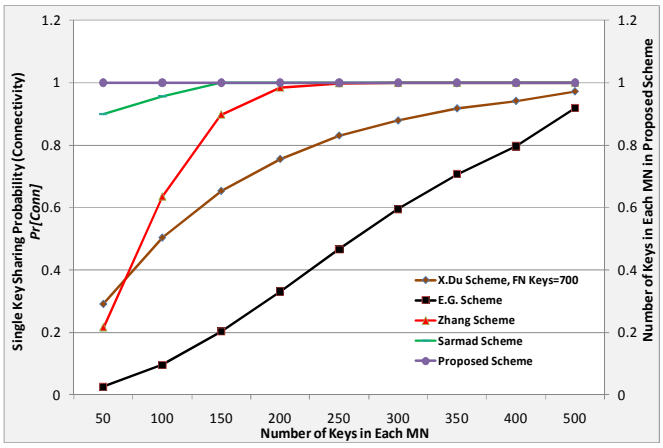

Figure 3. Probability of sharing at least one common key (Connectivity)

B. Memory Cost

This section presents the comparison of memory overhead of the proposed scheme with some well known existing key management schemes for HSNs.

In an ECC-based key management scheme [8], the total memory overhead is $(n_{MN}+3)*n_{FN}+2n_{MN}$, where n_{MN} and n_{FN} are the numbers of MNs and FNs respectively [32]. Instead, in the solution presented by Yang et al. [20], each FN is preloaded with a pair of public/private keys and $n_{FN}-1$ distinct pairwise keys, while no key is pre-loaded in the MNs. The memory overhead of this scheme is $(2+n_{FN}-1)*n_{FN}$. According to the basic scheme [12], each node is loaded with q keys before deployment, thus resulting in a total memory overhead of $q*(n_{FN}+n_{MN})$.

In the scheme proposed in this paper, each MN is loaded with only 3 keys (i.e., SK, K_{plc} and Authentication Key) and each FN is loaded with 6 keys (i.e., the BS public key, its own public/private key pair, SKG, CNDK and K_{prt}). The resulting memory overhead is $6n_{FN}+3n_{MN}$.

To analyze and compare the proposed scheme with the existing schemes [8, 12, 17, 20, 26], it is assumed that each FN is able to make a maximum of d connections with its neighboring MNs. According to [12], [17] and [26], if a node has N_c neighbors and that node has to establish secure links with only d neighbors, then the required key sharing probability should be

$$Pr = d / N_c \qquad (5)$$

For example, the single key sharing probability required to make 30 connections with the neighboring MNs out of 38 neighbors is approximately 0.80. From fig. 3, each node in [12] should carry 400 keys and each FN in [17] should carry 700 keys while each MN should carry 228 keys while in [26] each FN should carry 250 keys and each MN should carry 30 keys. In our scheme, each FN should be loaded with only 6 secret keys.

Fig. 4 summarizes the performance offered by different solutions in terms of the total number of the keys deployed for different sizes of the WSN. The results show that the proposed scheme requires fewer keys compared to other approaches. For less dense networks, the proposed scheme and Yang's scheme require almost the same number of keys. However, the proposed scheme performs better in dense networks.

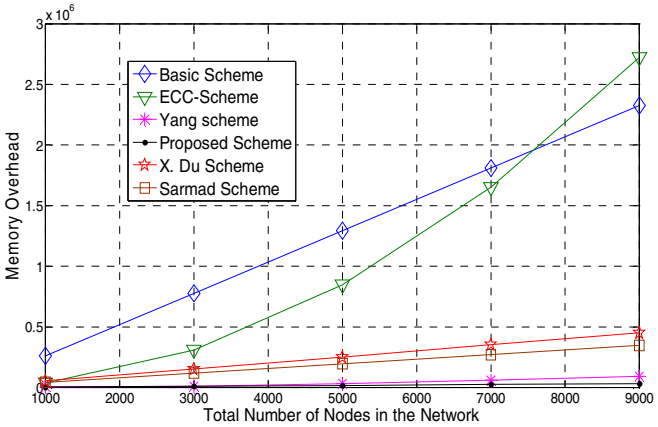

Figure 4. Comparison of memory overhead produce by the proposed scheme with some existing scheme

C. *Network Resilience to Node Compromised Attacks*

This section shows the effect of node compromised attacks on data communication capabilities. In the proposed scheme, FNs and MNs are provided with different security measures dealing with such attacks. Since FNs act as both CHs and data sinks for MNs, they are provided with tamper resistant hardware to protect their security material. Once the FN is captured, all security keys are replaced by a reference "compromised key" which does not allow the node to authenticate itself to the BS nor to accept any joining MN. On the contrary, MNs are not provided with the tamper resistant hardware.

Node compromised attack in case of balanced and unbalanced key pre-distribution schemes for homogeneous and heterogeneous sensor networks have a significant impact on the security offered by the communication links operating within the network due to the large number of shared keys with other nodes in the network. The fraction of communications compromised by compromising n MNs in shared key pre-distribution schemes is given by

$$Pr[Compromised] = 1 - (1 - \frac{K}{P})^n \qquad (6)$$

where K is the number of keys assigned to each MN from a pool of P keys. In case of compromised FNs, K is replaced by S in (6). Fig. 5 shows the OMNET++ simulation results about how many communications links a compromised MN can create with uncompromised MNs without involving the CH/FN. More specifically, the figure compares the proposed scheme with the schemes proposed in [12], [17], [26] and [29] with $Pr[Conn]$=0.8. The proposed scheme performs better because (i) a MN cannot establish directly a communication link with the other MNs of the network and (ii) all the FNs use the algorithm proposed in [28] to detect the compromised MNs.

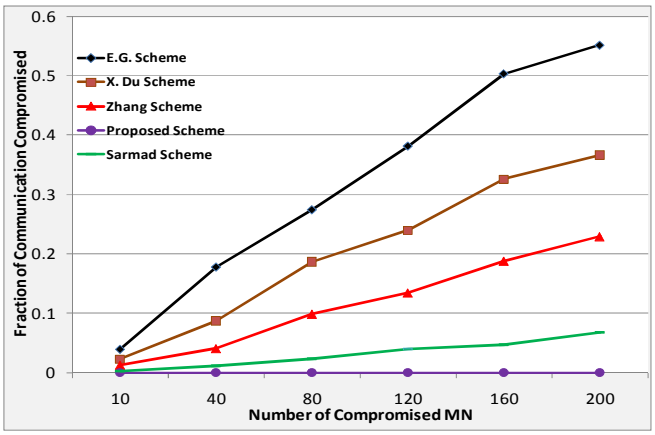

Figure 5. Fraction of communication compromised by capturing 'n' Mobile Nodes (MNs)

Since the FNs act as trusted servers to the MNs, their compromission can severely affect the network security. Fig. 6 shows a comparison of the OMNET++ simulation results for the FNs compromission of the proposed scheme with [12], [17] and [29]. It is clear from fig. 6 that FN compromission results in almost the same number of compromised links when using [12] and [17]. Although [29] proposed a balanced key distribution for the HSNs like [12] for homogeneous sensor networks, it performs better than [12] and [17] because it divides the key pool P into a number of groups equal to the number of clusters thus increasing not only network connectivity but also network resilience against both FN and MN capture attacks.

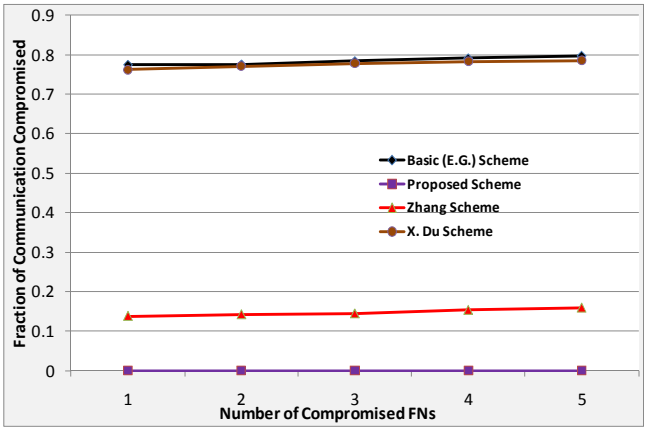

Figure 6. Fraction of communication compromised by capturing 'n' Fixed Nodes (FNs)

D. *Communication Overhead*

In this section, the communication overhead is evaluated also analyzing the different contributions from authentication

and key establishment phases. The simulation scenario is modified in order to include 16 FNs and 500 MNs.

a. Authentication Overhead

Concerning the authentication overhead, the total number of packets exchanged during the authentication phase is considered. The authentication phase of the proposed solution is compared with some of the existing approaches ([30], [31] and [32]). OMNET++ simulation results show that the proposed scheme produces less authentication overhead than the existing schemes, as shown in fig. 7.

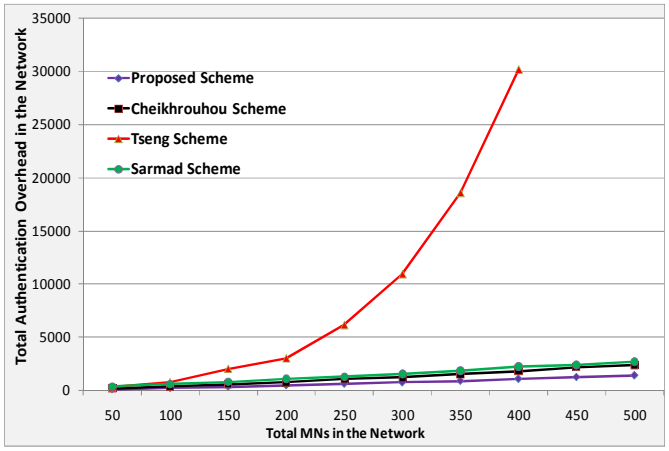

Figure 7. Authentication overhead comparison

b. Key Establishment Overhead

The proposed solution is also compared with the basic homogeneous [12] and heterogeneous [17, 32] schemes. The results show a significant reduction of the communication overhead. A 99% network connectivity probability for [12] and [17] was taken into account, computing the number of keys required in each FN and MN (using the results of (3) and (4)). The obtained results are shown in fig. 8. There is only a slight difference in terms of communication overhead between the homogeneous and heterogeneous approach, but there is a big difference in terms of memory cost (fig. 4).

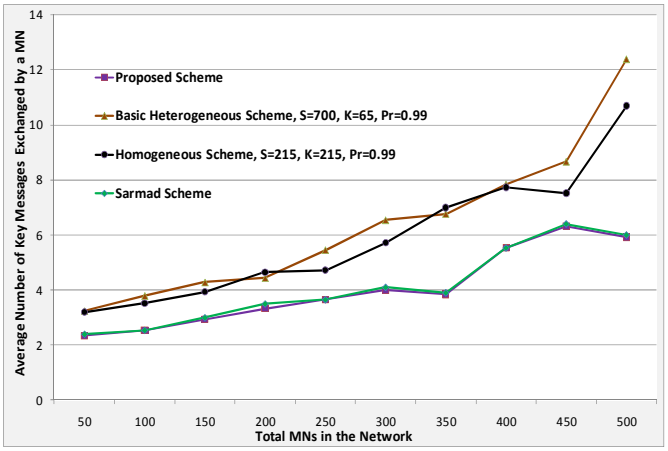

Figure 8. Average number of key messages exchanged during the first key establishment phase

c. Total Initialization phase Overhead

This section presents the OMNET++ simulation results for the total communication overhead generated during the first authentication and key establishment phase. The results of the proposed scheme have been compared with the ones related to [30] and [32], since both solutions are based on the mutual authentication and key establishment phases. Figure 9 represents the resulting communication overhead by varying the size of the network.

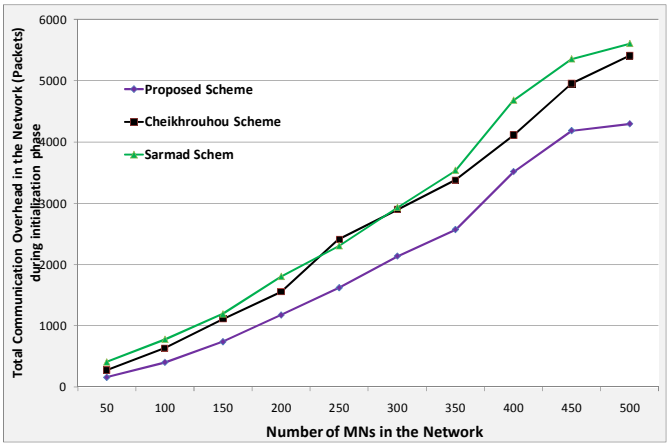

Figure 9. Total communication overhead in the network during the initialization phase

E. Energy Consumption

This section describes the average energy consumption of each node during the authentication and initialization phases of the network (again using the OMNET++ simulator). The proposed solution requires only 2 messages for the authentications as shown in fig. 7 compared to [31] which requires 4 messages and with [30, 32] which require 3 messages for authentication. The average energy consumption of each node during the authentication phase in the proposed scheme compared with [30], [31] and [32] is shown in fig 10.

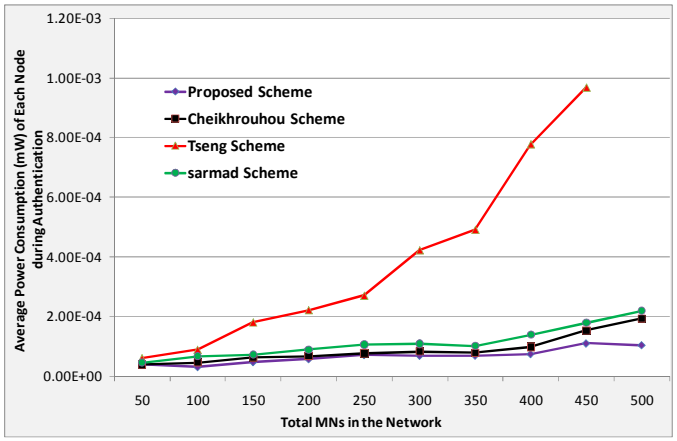

Figure 10. Average energy consumption of each node during the authentication phase

Fig. 9 also shows the effectiveness of combining the authentication and key establishment phases to reduce the total overhead during the initialization phase. Such optimization results in power savings at each node and in an overall

increase of the network life time. Fig. 11 represents the OMNET++ results for the average energy consumption of each node during the initialization phase (authentication and key establishment) in the proposed scheme, as compared with [30] and [32]. The results show that the proposed solution of combining the authentication and key establishment messages reduces the energy consumption with respect to [30, 32] where separate messages are exchanged for key establishment between the nodes after their successful authentication.

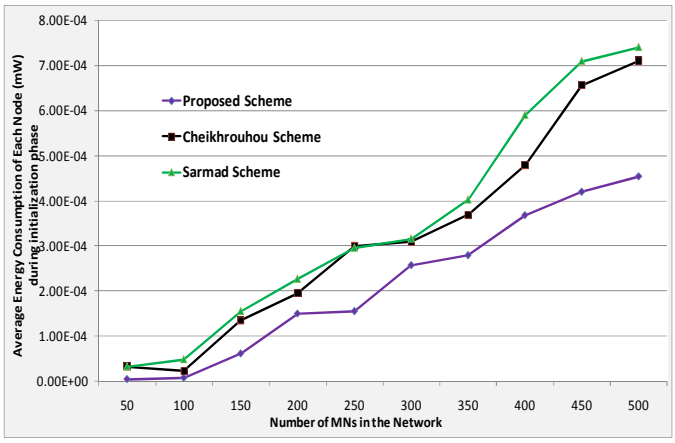

Figure 11. Average energy consumption of each node during the initialization phase

V. CONCLUSIONS

In this paper, a key management scheme is proposed for cluster-based heterogeneous sensor networks. In comparison with existing approaches, the proposed solution provides better network connectivity, reduces memory overhead, increases network resilience against node capture attacks and requires minimum communication overhead during the authentication and key establishment phases. Hence it saves battery energy and increases the network life time. In this paper, only intra network movements of the mobile nodes were considered. Future work will analyze inter networks mobility scenarios.

REFERENCES

[1] M. O. Rabin. Digitalized signatures and public-key functions as intractable as factorization. Technical Report MIT/LCS/TR-212, Laboratory for Computer Science, MIT, 1979.

[2] Gupta, P.; Kumar, P.R.; , "The capacity of wireless networks," *Information Theory, IEEE Transactions on* , vol.46, no.2, pp.388-404, Mar 2000.

[3] Kaixin Xu; Xiaoyan Hong; Gerla, M.; , "An ad hoc network with mobile backbones," *Communications, 2002. ICC 2002. IEEE International Conference on* , vol.5, no., pp. 3138- 3143 vol.5, 2002.

[4] L. Girod, T. Stathopoulos, N. Ramanathan, et al., "A System for Simulation, Emulation, and Deployment of Heterogeneous Sensor Networks", Proc. of ACM SenSys 2004.

[5] Yi Cheng; Agrawal, D.P.; , "Efficient pairwise key establishment and management in static wireless sensor networks," *Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on* , vol., no., pp.7 pp.-550, 7-7 Nov. 2005.

[6] Duarte-Melo, E.J.; Mingyan Liu; , "Analysis of energy consumption and lifetime of heterogeneous wireless sensor networks," *Global Telecommunications Conference, 2002. GLOBECOM '02. IEEE* , vol.1, no., pp. 21- 25 vol.1, 17-21 Nov. 2002.

[7] Fang Liu, Maiou Jose "Manny " Rivera, Xiuzhen Cheng, "Location-Aware Key Management in wireless sensor networks", IWCMC'06, 2006.

[8] Xiaojiang Du; Yang Xiao; Song Ci; Guizani, M.; Hsiao-Hwa Chen; , "A Routing-Driven Key Management Scheme for Heterogeneous Sensor Networks," *Communications, 2007. ICC '07. IEEE International Conference on* , vol., no., pp.3407-3412, 24-28 June 2007.

[9] E. J. Duarte-Melo and M. Liu, "Data-gathering Wireless Sensor Networks: Organization and Capacity", Computer Networks (COMNET) Special Issue on Wireless Sensor Networks, Vol. 43, Issue 4, November 2003, pp. 519-537.

[10] Seshadri, A.; Perrig, A.; van Doorn, L.; Khosla, P.; , "SWATT: softWare-based attestation for embedded devices," *Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on* , vol., no., pp. 272- 282, 9-12 May 2004.

[11] Yarvis, M.; Kushalnagar, N.; Singh, H.; Rangarajan, A.; Liu, Y.; Singh, S.; , "Exploiting heterogeneity in sensor networks," *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE* , vol.2, no., pp. 878- 890 vol. 2, 13-17 March 2005.

[12] L. Eschenauer and V. D. Gligor, "A key management scheme for distributed sensor networks", Proc. of the 9th ACM Conference on Computer and Communication Security, Nov. 2002. pp. 41-47.

[13] Haowen Chan; Perrig, A.; Song, D.; , "Random key predistribution schemes for sensor networks," *Security and Privacy, 2003. Proceedings. 2003 Symposium on* , vol., no., pp. 197- 213, 11-14 May 2003

[14] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, M. Yung, "Perfectly Secure Key Distribution for Dynamic Conferences", (1992) 471–486.

[15] Camtepe, S.A.; Yener, B.; , "Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks," *Networking, IEEE/ACM Transactions on* , vol.15, no.2, pp.346-358, April 2007.

[16] A. Perrig, R. Szewczyk, J. Tygar, Victorwen, and D. E. Culler, "Spins: Security Protocols for Sensor Networks", ACM Wireless Networking, Sept. 2002.

[17] Du. X., Xiao, Y., Guizani, M. Chen, H. H., "An effective key management scheme for heterogeneous sensor networks", Ad Hoc Networks, Vol. 5 No. 1, 2007, pp. 24-34.

[18] Sanchez, D.S.; Baldus, H.;"A Deterministic Pairwise Key Pre-distribution Scheme for Mobile Sensor Networks," *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on* , vol., no., pp. 277- 288, 05-09 Sept. 2005.

[19] S.Hussain, F.Kausar, and A.Masood, "An Efficient Key Distribution Scheme for Heterogeneous Sensor Networks", IWCMC'07, 2007.

[20] Qing Yang; Qiaoliang Li; Sujun Li; , "An Efficient Key Management Scheme for Heterogeneous Sensor Networks," *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on* , vol., no., pp.1-4, 12-14 Oct. 2008.

[21] Poornima, A.S.; Amberker, B.B.; , "Tree-based key management scheme for heterogeneous sensor networks," *Networks, 2008. ICON 2008. 16th IEEE International Conference on* , vol., no., pp.1-6, 12-14 Dec. 2008.

[22] Juwei Zhang,; Yugeng Sun,; Liping Liu,; , "NPKPS: A novel pairwise key pre-distribution scheme for wireless sensor networks," *Wireless, Mobile and Sensor Networks, 2007. (CCWMSN07). IET Conference on* , vol., no., pp.446-449, 12-14 Dec. 2007.

[23] Kyeong Tae Kim; Ramakrishna, R.S.; , "A Level-based Key Management for both In-Network Processing and Mobility in WSNs," *Mobile Adhoc and Sensor Systems, 2007. MASS 2007. IEEE Internatonal Conference on* , vol., no., pp.1-8, 8-11 Oct. 2007.

[24] I-Hsun Chuang; Wei-Tsung Su; Chun-Yi Wu; Jang-Pong Hsu; Yau-Hwang Kuo; , "Two-Layered Dynamic Key Management in Mobile and Long-Lived Cluster-Based Wireless Sensor Networks," *Wireless Communications and Networking Conference, 2007.WCNC 2007. IEEE* , vol., no., pp.4145-4150, 11-15 March 2007.

[25] Kamendje, G.-A.; , "A tamper resistant CMOS crypto-key generation unit," *Circuits and Systems, 2002. ISCAS 2002. IEEE International Symposium on* , vol.2, no., pp. II-352- II-355 vol.2, 2002.

[26] Sarmad, U.K.; Lavagno, L.; Pastrone, C.; , "A key management scheme supporting node mobility in heterogeneous sensor networks," *Emerging Technologies (ICET), 2010 6th International Conference on*, vol., no., pp.364-369, 18-19 Oct. 2010.

[27] Maerien, J.; Michiels, S.; Huygens, C.; Joosen, W.; , "MASY: MAnagement of Secret keYs for federated mobile wireless sensor networks," *Wireless and Mobile Computing, Networking and Communications (WiMob), 2010 IEEE 6th International Conference on* , vol., no., pp.121-128, 11-13 Oct. 2010.

[28] Xinyu Jin; Putthapipat, P.; Deng Pan; Pissinou, N.; Makki, S.K.; , "Unpredictable Software-based Attestation Solution for node compromise detection in mobile WSN," *GLOBECOM Workshops (GC Wkshps), 2010 IEEE* , vol., no., pp.2059-2064, 6-10 Dec. 2010

[29] Zhang Juwei; Zhang Liwen; , "A Key Management Scheme for Heterogeneous Wireless Sensor Networks Based on Group-Oriented Cryptography," *Internet Technology and Applications, 2010 International Conference on* , vol., no., pp.1-5, 20-22 Aug. 2010.

[30] Cheikhrouhou, O.; Kouba□a, A.; Boujelben, M.; Abid, M.; , "A lightweight user authentication scheme for Wireless Sensor Networks," *Computer Systems and Applications (AICCSA), 2010 IEEE/ACS International Conference on* , vol., no., pp.1-7, 16-19 May 2010

[31] Huei-Ru Tseng; Rong-Hong Jan; Wuu Yang; , "An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks," *Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE* , vol., no., pp.986-990, 26-30 Nov. 2007.

[32] Khan, Sarmad Ullah; Lavagno, Luciano; Pastrone, Claudio; Spirito, Maurizio; , "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.