Secure Wireless Sensor Networks: Problems and Solutions

Fei Hu * Jim Ziobro ** Jason Tillett * Neeraj K. Sharma ******

* IEEE Member {fei.hu@ieee.org}, Computer Engineering Department, Rochester Institute of Technology, Rochester, New York 14623, USA
** IEEE Senior Member {j.ziobro@ieee.org}, Computer Engineering Department, Rochester Institute of Technology, Rochester, New York 14623, USA
*** Senior Researcher {jtillett@netsup.net}, Laboratory for Autonomous Cooperative Microsystems College of Engineering, RIT
**** IEEE Senior Member {sharman@clarkson.edu}, Electrical & Computer Engineering Department, Clarkson University, Potsdam, New York 13699, USA

ABSTRACT

As sensor networks edge closer towards wide-spread deployment, security issues become a central concern. So far, the main research focus has been on making sensor networks feasible and useful, and less emphasis was placed on security. This paper analyzes security challenges in wireless sensor networks and summarizes key issues that should be solved for achieving the ad hoc security. It gives an overview of the current state of solutions on such key issues as secure routing, prevention of denial-of-service and key management service. We also present some secure methods to achieve security in wireless sensor networks. Finally we present our integrated approach to securing sensor networks.

Keywords: Sensor networks, wireless networks, security

1. INTRODUCTION

Very energy-efficient, scaleable, and strong security services including confidentiality, integrity, and group-level authentication of sensor data and routing control traffic are needed. Although significant progress has been shown in developing Wireless Sensor Networks (WSN) in many aspects including topology management, routing algorithm, MAC protocol and sensor data management (please refer to a comprehensive review on WSN in [1]), very little work is done on securing WSN. Research into authentication and confidentiality mechanisms designed specifically for WSN is needed. To understand the serious limitations of current security mechanisms, it is necessary to realize the salient differences between WSN and general ad-hoc networks[1] since some proposals were already raised for securing ad-hoc networks [7-9].

The features of WSN such as low-memory, low-energy and large-scale nodes make it impractical to use the majority of the current secure algorithms that were designed for powerful workstations. For example, the working memory of a sensor node is insufficient to even hold the variables (of sufficient length to ensure security) that are required in asymmetric cryptographic algorithms [4].

The first challenges of security in sensor networks lie in the conflicting interest between minimizing resource consumption and maximizing security. Therefore the usefulness of a potential solution depends how good the compromise it achieves is. The *resource* in this context includes energy as well as computational resource like CPU cycles, memory, communication bandwidth. As stated in the Introduction section, any security mechanisms for WSN should take the following has five major resource constraints into consideration: (1) limited energy, (2) limited memory, (3) limited computing power, (4) limited communication bandwidth, (5) limited communication range; more or less in descending order of acuteness.

Secondly, the capabilities and constraints of sensor node hardware will influence the type of security mechanisms that can be hosted on a sensor node platform. Since the amount of additional energy consumed for protecting each message is relatively small, the greatest consumer of energy in the security realm is key establishment [3].

Thirdly, the ad-hoc networking topology renders a WSN susceptible to link attacks ranging from passive eavesdropping to active interfering. Unlike fixed hardwired networks with physical defense at firewalls and gateways, attacks on a WSN can come from all directions and target at any node. Damage can include leaking secret information, interfering message and impersonating nodes, thus violating the above security goals.

Fourthly, the wireless communication characteristics of WSN render traditional wired-based security schemes impractical. Table 2 lists salient networking features of WSN and their corresponding impacts on security design.

Based on the above analysis on the security challenges, challenges and potential attacks in WSN, we further summarize three key issues for achieving the

[1] Wireless Sensor Networks is usually classified as a type of ad-hoc networks that can be defined as follows [10]: An ad hoc network is a collection of autonomous nodes or terminals that communicate with each other by forming a multi-hop radio network and maintaining connectivity in a decentralized manner; there is no fixed infrastructure such as base station or mobile switching in ad-hoc networks.

security of ad hoc networks:

(1) **Key Management in WSN**

Confidentiality, integrity, and authentication services are critical to preventing an adversary from compromising the security of a WSN. Key management is likewise critical to establishing the keys necessary to provide this protection in WSN. However, providing key management is difficult due to the ad hoc nature, intermittent connectivity, and resource limitations of the sensor network environment.

Traditional key management service is based on a trusted entity called a certificate authority (CA) to issue public key certificate of every node. The trusted CA is required to be online in many cases to support public key revocation and renewal. But it is dangerous to set up a key management service using a single CA in a sensor network. The single CA will be the vulnerable point of the network. If the CA is compromised, the security of the entire network is crashed. How to set up a trusted key management service for the WSN is a big issue.

(2) Securing routing of WSN

There are two kinds of threats to ad hoc routing protocols [15]: (1) External attackers. The attacks include injecting erroneous routing information, replaying old routing information, and distorting routing information. Using these ways, the attackers can successfully partition a network or introduce excessive traffic load into the network, therefore cause retransmission and ineffective routing. Using cryptographic schemes, such as encryption and digital signature can defend against the external attacks. (2) Internal compromised nodes. They might send malicious routing information to other nodes. It is more severe because it is very difficult to detect such malicious information because compromised node can also generate valid signature.

Existing routing protocols cope well with the dynamic topology, but usually offer little or no security measures [8]. An extra challenge here is the implementation of the secured routing protocol in a network environment with dynamic topology, vulnerable nodes, limited computational abilities and strict power constrains.

(3) Prevention of Denial-of-service

Strictly speaking, although we usually use the term Denial-of-service (DoS) to refer to an adversary's attempt to disrupt, subvert, or destroy a network, a DoS attack is any event that diminishes or eliminates a network's capacity to perform its expected function. Hardware failures, software bugs, resource exhaustion, environmental conditions, or any complicated interaction between these factors can cause a DoS.

An adversary may possess a broad range of DoS attack capabilities in WSN. For example, a wireless sensor network can be aerially deployed in enemy territory. If the enemy already has a wired network and power grid available and can interact with the newly deployed sensor network, it can apply powerful back-end resources to subvert or disrupt the new network.

The following three sections will further discuss the abovementioned three issues from three aspects: problem description, current research status and our suggested approach. In section 6 we will present our integrated approach to secure WSN.

3. Key Management in WSN

3.1 Problem description

Most of the security mechanisms require the use of some kind of cryptographic keys that need to be shared between the communicating parties. The purpose of key management is to [31]:

- Initialize system users within a domain.
- Generate, distribute and install keying material.
- Control the use of keying material.
- Update, revoke and destroy keying material.
- Store, backup/recover and archive keying material.

But key management is an unsolved problem in WSN. Traditional Internet style key management protocols based on infrastructures using trusted third parties are impractical for large scale WSNs because of the unknown network topology prior to deployment and serious node constraints such as limited power and limited transmission range.

At the extremes, there are *network-wide pre-deployed keying* and *node-specific pre-deployed keying* in sensor networks [36]. Generally speaking, the problem of key management in WSN can be decomposed into the following sub-problems:

- Key Pre-distribution:

To date, the only practical options for the distribution of keys to sensor nodes in WSN whose topology is unknown prior to deployment will have to rely on key pre-distribution [37]. Keys have to be installed in sensor nodes to secure communications. However, traditional key-distribution schemes have the following shortcoming: either a single *mission key* or a set of separate *n-1* keys, each being pair-wise privately shared with another node, have to be installed in every sensor node. In key pre-distribution, a big issue is how to load a set of keys (called key ring) into the limited memory of each sensor. Other problems include the saving of the key identifier of a key ring and associating sensor identifier with a trusted controller node.

- Neighbor discovery:

Every node needs to discover its neighbors in wireless communication range with which it shares keys. Thus neighbor discovery is also called shared-key discovery that establishes the topology of the sensor array as seen by the routing layer of the WSN. A 'link' exists between two sensor nodes only if they share a key. Good neighbor discovery scheme will not give an

attacker any opportunity to discover the shared keys and thus the attacker can only do traffic analysis.

- End-to-end path-key establishment:

For any pair of nodes that do not share a key but are connected by multiple hops need to be assigned a path-key for end-to-end secure communication. Path-key cannot be the one already used by the shared keys between neighbor nodes.

- Isolating aberrant nodes:

An aberrant node is one that is not functioning as specified. Identifying and isolating aberrant nodes that are serving as intermediate nodes is important to the continued operation of the sensor network. A node may cease to function as expected for the following reasons [6]:

- It has exhausted its source of power.
- It is damaged by an attacker.
- It is dependent upon an intermediate node and is being deliberately blocked because the intermediate node has been compromised.
- An intermediate node has been compromised and it is corrupting the communication by modifying data before forwarding it.
- A node has been compromised and it communicates fictitious information to the base station.

- Re-keying:

Although it is anticipated that in most WSNs the lifetime of a key shared between two nodes exceeds that of the two nodes, it is possible that in some cases the lifetime of keys expires and re-keying must take place. Re-keying is a challenge issue since new keys needs to be generated in an energy-efficient way and the re-keying period should be determined based on the security level to be achieved. Re-keying is equivalent with a self-revocation of a key by a node.

- Key-establishment latency:

Recent investigation reveals that latency is potentially a significant impediment to secure network initialization [42]. As with energy consumption, latency due to communications is a much larger factor than computational latency. Thus any key management scheme should take latency reduction as a crucial factor.

3.2 Solutions

Currently there are some key management schemes that can be partially used for securing WSN environments even though most of those schemes are proposed for general ad hoc networks.

- Hybrid key-based protocols:

An obvious conclusion from current research results is that a single keying protocol will not be optimal for all sensor network topologies, densities, sizes, and scenarios. Protocols such as Identity-Based Symmetric Keying and Rich Uncle have limited application until the network's *routing infrastructure* has been sufficiently well established. Individually other protocols such as the public-key group and pairwise keying protocols consume too much energy. For *significant* sensor networks, a mix of public key-based protocols, including pairwise, group keying, and distribution keying, provide an energy-efficiency superior to using just a single protocol [3].

- Threshold cryptography:

A solution to deal with key management in general ad hoc networks is proposed by Zhou and Hass in [8] and may be borrowed to WSN environments. It uses a *(k, n)* threshold scheme to distribute the services of the certificate authority to a set of specialized server nodes. Each of these nodes is capable of generating a partial certificate using their share of the certificate signing key sk_{CA}, but only by combining k such partial certificates can a valid certificate be obtained. The solution is suitable for planned, long-term ad hoc networks. However, it may not be applicable for WSN because sensor networks can lose some nodes whose energy is run out of. In addition, [8] is based on public key encryption and thus requires that the all the nodes are capable of performing the necessary computations, which may not be feasible for energy-limited sensor nodes.

- Certificate repository:

Hubaux et al. [35] go a step further than [8], by requiring each node to maintain its own *certificate repository*. These repositories store the public certificates that the node themselves issue, and a selected set of certificates issued by the others. The *performance* is defined by the probability that any node can obtain and verify the public key of any other user, using only the local certificate repositories of the two users. The dilemma is: too many certificates in a sensor node would easily exceed their capacity, yet too few might greatly impact the performance (as previously defined) of the entire network.

- Fully Distributed Certificate Authority

Fully Distributed Certificate Authority is first described by Luo and Lu in [32] and later analyzed by Luo et al in [9] and [33]. Its uses a *(k, n)* threshold scheme to distribute an RSA certificate signing key to all nodes in the network. It also uses verifiable and proactive secret sharing mechanisms to protect against denial of service attacks and compromise of the certificate signing key. Since the service is distributed among all the nodes when they join the network, there is no need to elect or choose any specialized server nodes. Similar to the solution presented in [8], this solution is aimed towards planned, long-term ad hoc networks with nodes capable of public key encryption and thus could not adapt the routing changing of sensor networks.

- Pebblenets:

Secure Pebblenets proposed by Basagni et al [5] provides a distributed key management system based on symmetric encryption. The solution provides group authentication, message integrity and confidentiality. This solution is suitable for planned and distributed,

long-term ad hoc networks consisting of low performance nodes that are unable to perform public key encryption. We hold the same opinion as [34] and believe that this solution can provide more practical security scheme for sensor networks. Pebblenets use only symmetric cryptography. The disadvantage is that once a node is compromised, forward secrecy is broken, therefore tamper- resistance becomes crucial. of *threshold cryptography* [45, p. 71]. In addition, in pebblenets a key management server not only has to store its own key pair, but also the public keys of all the nodes in the network. The difficulty includes the storage requirement exerted on the servers which must potentially be specialized nodes in the network, and the overhead in signing and verifying routing message both in terms of computation and of communication.

4. SECURE ROUTING IN WSN

4.1 Problem description

There are many new routing protocols proposed for ad hoc networks and some of them can be used in WSN [38]. Among those routing protocols, the Ad hoc On-demand Distance Vector (AODV) protocol [39] and the Dynamic Source Routing (DSR) protocol [40] have recorded very good performance [41]. Unfortunately security issues arise with these protocols, because security features are not designed built-in [49].

We can further formulate the secure WSN routing problem as follows: *Denote A,B as* principals, such as communicating nodes; and *KAB* and *KBA* denote the secret MAC keys shared between *A* and *B* (one key for each direction of communication). MAC*KAB*(*M*) denotes the computation of the message authentication code (MAC) of message *M* with the MAC key *KAB*. We need to solve the following problems for secure WSN routing protocols:

(1) An *authentication mechanism* with low computation and communication overhead is needed to prevent an attacker from performing a Denial-of-Service (DoS) attack by flooding nodes with malicious messages, overwhelming them with the cost of verifying authentication. For instance, for point-to-point authentication of a message, we may use a message authentication code (MAC) and a shared key between the two parties [50].

(2) Secure *Route Discovery*. Assume that the initiator *A* performs a Route Discovery for target *B*, and that they share the secret keys *KAB* and *KBA*, respectively, for message authentication in each direction. Route Discovery mechanism should enable the target to verify the authenticity of the Route Requestor; It also needs to authenticate data in route request messages and route reply messages through the using of *KAB* and *KBA*. Malicious nodes may be avoided during Route Discovery. For example, Each Route Request Message can include a list of nodes to avoid, and the MAC that forms the initial hash chain element is then computed over that list of nodes. Malicious nodes cannot add or remove nodes from this list without being detected by the target.

(3) *Route Maintenance*. A node forwarding a packet to the next hop along the source route returns a *route error message* to the original sender of the packet if it is unable to deliver the packet to the next hop after a limited number of retransmission attempts. It is a big issue to secure those *route error messages* and prevent unauthorized nodes from sending those messages.

(4) *Defending from Routing Misbehavior*: We need a means of determining whether intermediate nodes are in fact forwarding packets that they have been requested to forward. For example, watchdog and pathrater [18] attempt to solve this problem by identifying the attacking nodes and avoiding them in the routes used.

(5) *Defending from Flooding attack*: An active attacker can attempt to degrade the performance of DSR or other on-demand routing protocols by repeatedly initiating Route Discovery. In this attack, an attacker sends Route Request packets, which the routing protocol floods throughout the network. To protect the routing protocols from a flood of Route Request packets, we need a mechanism that enables nodes to instantly authenticate ROUTE Requests, so nodes can filter out forged or excessive Request packets. In [50] the authors introduce *Route Discovery chains*, a mechanism for authenticating Route Discoveries, allowing each node to rate-limit Discoveries initiated by any node.

4.2 Solutions

Some research work is done in order to secure ad hoc routing algorithm. For instance, a security-enhanced version of AODV called Security-aware AODV (SAODV) is introduced in [43]. It is claimed that SAODV achieves a satisfactory performance-overhead trade-off. However the fact that it is a metric-centric approach that relies on an user-defined, application-dependent parameter for evaluating trust level, does not solve the basis of the security problem and leaves a lot of questions to be answered. There are other approaches where *route redundancy* is the property that is mostly taken advantage of [44-45]. Besides security performance, energy consumption raises concern about the practicability of a particular protocol since energy is the most important factor in WSN.

The above approaches to securing routing are most applicable to general ad hoc networks. However, their ideas can be partially used to secure WSN routing. So far there are only a few proposals that are raised specifically for securing routing of sensor networks. We summarize their features as follows:

- **SPINS**

SPINS (Security Protocols for Sensor Networks) is one of the exceptions where routing is an application of a security framework [4]. SPINS comprised of *Sensor Network Encryption Protocol* (SNEP) and μTESLA. The function of SNEP is to provide confidentiality (privacy), two-party data authentication, integrity and freshness. μTESLA is to provide authentication to data broadcasts.

❑ **Ariadne**

Ariadne [46,50] absorbs the ideas of SPINS and came out with a hardened version of DSR. One of the requirements is that every node has to be able to generate an one-way key chain. Since the memory of a sensor node is limited, it cannot afford to generate a long key chain, and so has to spend a lot of time generating keys. By enforcing authenticity alone, Ariadne does not guard against attacks by multiple colluding nodes.

❑ **INSENS**

A recent solution called INSENS (INtrusion-tolerant routing protocol for wireless SEnsor NetworkS) for securing WSN routing is proposed in [48]. An important property of INSENS is that while a malicious node may be able to compromise a small number of nodes in its vicinity, it cannot cause widespread damage in the network.

5. Prevention of Denial-of-Service attacks in WSN

In Denial-of-Service (DoS) attacks, the hacker's objective is to render target machines inaccessible by legitimate users. WSN without sufficient protection from DoS attacks may not be deployable in many areas. Apart from special cases whereby an a priori trust exists in all nodes, the nodes of an ad hoc sensor network cannot be trusted for the correct execution of critical network functions. Essential network operations that assure basic connectivity can be heavily jeopardized by nodes that do not properly execute their share of the network operations like routing, packet forwarding, name-to-address mapping, and so on. Node misbehavior that affects these operations may range from simple selfishness or lack of collaboration due to the need for power saving to active attacks aiming at denial of service (DoS) and subversion of traffic. There are two types of DoS attacks [16]:

- *Passive attacks:* Selfish nodes use the network but do not cooperate, saving battery life for their own communications: they do not intend to directly damage other nodes.
- *Active attacks:* Malicious nodes damage other nodes by causing network outage by partitioning while saving battery life is not a priority.

DoS attacks can happen in multiple WSN protocol layers [11].

There is very little work done on the prevention of DoS attacks. Attempts to add DoS resistance to existing protocols often focus on cryptographic-authentication mechanisms. Aside from the limited resources that make digital-signature schemes impractical, authentication in sensor networks poses serious complications.

Currently there are four mechanisms that could be helpful to overcome DoS attacks in WSN:

- Watchdog scheme:

Based on the above analysis, we can see that a necessary operation to overcome DoS attacks is to identify and circumvent the misbehaving nodes. Watchdog scheme attempts to achieve this purpose through the using of two concepts: *watchdog* and *pathrater* [18].

- Rating scheme:

Watchdog scheme was further investigated and extended to rating scheme [19-21]. In rating scheme the neighbors of any single node collaborate in rating the node, according to how well the node execute the functions requested from it.

- Virtual currency:

This scheme conceptualized the motivation for nodes not to be selfish as *nuglets*, a sort of virtual currency (also called nuglets) [22,23].

- Route DoS prevention:

This scheme attempts to prevent DoS in the routing layer through the cooperation of multiple nodes. In [24] the authors introduce a mechanism to assure routing security, fairness and robustness targeted to mobile ad hoc networks. In [25], the authors proposed levels of protection as a negotiable metric in route discovery. In this way, a pair of nodes establishes a certain application-specific level of protection before any security-sensitive traffic begins.

6. Our proposed approach

Our proposed sensor network security scheme includes four phases (see Figure 1).

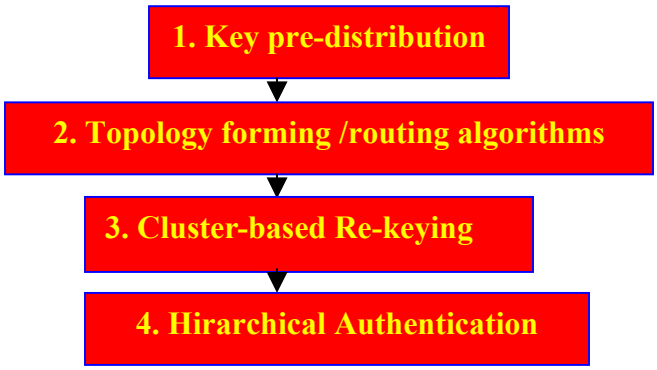

Figure 1. Integration security with routing

The reasons that we suggest the above security steps are as follows:

(1) Phase 1 principle (key pre-distribution): To

achieve security, communication should be encrypted and authenticated. The open problem is how to bootstrap secure communications between sensor nodes, i.e. *key agreement* problem. There are currently three types of general key agreement schemes: trusted-server schemes, self-enforcing schemes, and key pre-distribution schemes. *Trusted-server* schemes depend on a trusted server for key agreement between nodes; which is not suitable for sensor networks because in an ad hoc network scenario one cannot generally assume any trusted infrastructure. *Self-enforcing* schemes depend on asymmetric cryptography; an example is an authenticated key agreement protocol using public-key certificates. However, as pointed out in [72], the limited computation and energy resources of sensor nodes often make it undesirable to use public-key algorithms. The third type of key agreement scheme is key *pre-distribution*, where key information is distributed to all sensor nodes prior to deployment. The third scheme is approved to be the only feasible one to bootstrap sensor network security transmission [76].

(2) Phase 2 principle (cluster-based routing forming): Although some key management schemes were proposed to generate paiwise keys [76] or global keys (key shared between base station and each sensor) [72], they ignored the specific architecture characteristics of sensor networks as follows:

- The biggest concern in sensor networks is energy. Most energy is consumed in communication instead of local procession [72]. To save communication overhead, data aggregation in some immediate sensors are necessary. Thus each sensor should not only share a global key with the base station (sink) but also share "link" keys with the aggregation sensors. How to choose aggregation sensors in a large-scale and dynamic sensor network? How to generate "link" keys periodically? Current security schemes do not address these problems.
- We argue that a practical security scheme should be based on an energy-efficient routing scheme. We thus propose a cluster-based routing architecture after key pre-distribution and sensor deployment. Our cluster-based scheme is different from current routing algorithms such as ZRP [78] and LEACH [77]. To save energy, we suggest a minimum spanning tree topology organization in each cluster. Between clusters we adopt con-centric cost-level architecture to find out a reliable data forwarding path. For our detail routing algorithm please refer to [79].

(3) Phase 3 principle (re-keying): Many sensor networks have dynamic topology such as battlefield monitoring, traffic control and animal habitat study. The enemies may capture some sensors. New sensors can be added to an existing network for compensating the dead sensors that run out-of-power. Therefore periodically we need to update the keys. Most security schemes ignore the importance of re-keying scheme. We propose the updating procedure of two types of keys in sensor networks: cluster key and pairwise key. We also calculate the re-keying period according to sensors' mobility feature.

(4) Phase 4 principle (Hirarchical Authentication): One of the most important problems in sensor networks is "broadcast authentication" problem. That is, if an attacker declares itself as a legal base station and broadcast false commands to the sensors, how do we identify such phony packets? In [72], a low-energy broadcast authentication scheme is proposed. However, it does not adapt to the following situation: if the lifetime of a sensor network is much larger than each authentication interval, we will have a long key chain and intensified key calculations.

6.1 Phase 1: Key pre-distribution:

The first step of our integrated security scheme is key pre-distribution. We already provided the reason of this phase in last section.

Suppose we drop a bunch of sensors from the plane to a battlefield, how can we make sure any of two sensors can find a shared key to encrypt/decrypt their messages, i.e. they have a pairwise key? Please notice we cannot use public key (Asymmetric approach) scheme to secure transmission since the limited memory of a sensor cannot even hold a public key that is typically a few thousand bytes [72]. Currently two schemes are proposed to address key pre-distribution problem in sensor networks: key-pool approach [73] and probabilistic approach [76]. We prefer the latter approach since it needs too much memory and calculation overhead of we build a key chain in each sensor and make sure any two sensors share a key at (at least) 50% probability. We also suggest the using of Blom scheme [75,80] to generate a temporary matrix when two sensors need to build a secure channel. Blom scheme just needs a 'seed' (it can be the sensor ID) pre-stored in each sensor. Each seed can generate a matrix over a finite field. If there is a common space between two matrixes, a shared key can be found out [80].

6.2 Phase 2: self-organizing sensors to a cluster-based topology and routing architecture

After sensors are deployed randomly in an area, to reduce key generation overhead (a flat topology can lead an exponential increase of pairwise key generation frequency with the incrase of network density [68]), we choose some sensors to become cluster heads based on "Voronoi Tessellation theory" [79]. The choosing

probability decreases with the increase of sensor density (Fig.2). After some sensors declare themselves as cluster heads, they send 'hello' messages to the neighboring sensors to form clusters. Inside each cluster, we adopt Minimum Spanning Tree (MST) algorithm to maintain a connected intra-cluster topology. Detail MST algorithm is in [79].

Between different clusters, to find out low-energy secure path, we propose a con-centric topology forming architecture [79], each cluster head maintains a cost level that is determined by the hop number and required communication energy consumption between itself and base station.

Figure 4 clearly shows that our cluster-based routing scheme can greatly save communication overhead compared to other sensor network routing schemes such as LEACH and ZRP.

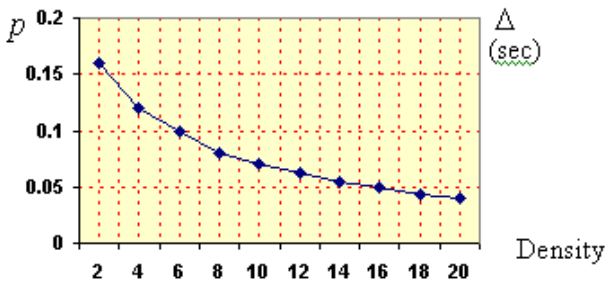

Fig. 2: cluster-head choosing probability ~ sensor

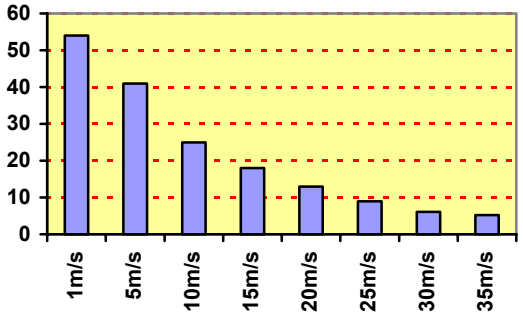

Fig. 3: re-keying period ~ speed

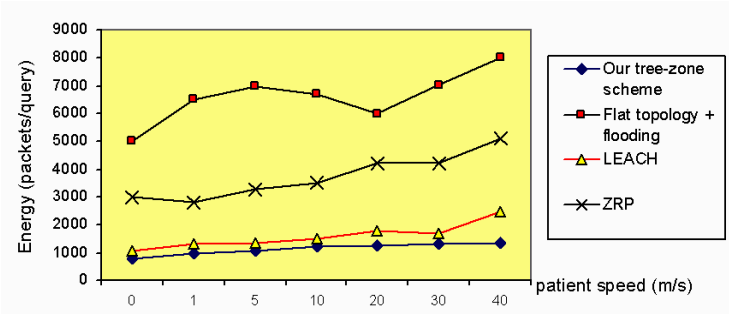

Figure 4. Our cluster topology saves energy

6.3 Phase 3: Re-keying

To adapt to the dynamic topology of sensor networks, we update keys (re-keying) periodically. The re-keying period is calculated based on the mobility factor [79] (see Fig.3).

In our re-keying scheme, we will update two keys: (1) Cluster keys which are shared between each cluster head and all its cluster members. Thus data aggregation security can be achieved through cluster keys; (2) Pairwise keys which are shared only between any two sensors themselves. Pairwise keys can be used to generate cluster keys.

$$u \longrightarrow * : \quad u, Nonce_u.$$
$$v \longrightarrow u : \quad v, MAC(K_v, Nonce_u|v)$$
$$K_{uv} = f_{K_v}(u)$$

Figure 5. Re-keying (for pairwise keys)

In each cluster, the cluster head broadcasts a 'hello' message including its ID and a 'nonce' (a sequence number used only once in the whole sensor network lifetime) to all the neighboring sensors. When a neighboring sensor receives this message, it feedbacks a Message Authenticated Code (MAC) encrypted by a pairwise key to the cluster head. Thus the cluster head can use a pseudo-random function to regenerate a new pairwise key between itself and this sensor (Fig.5).

Once all the 'pairwise keys' in a cluster are updated, the new 'cluster key' can be transmitted to each cluster member through the corresponding pairwise key.

6.4 Phase 4: Hierarchical Authentication

The last phase of our integrated security scheme is a new broadcast authentication scheme that addresses the following problem: if the lifetime of a sensor network is much larger than the interval of a μTESLA [72], how can we reduce the pseudo-random calculation overhead and key chain length in the whole broadcast authentication procedure. We cannot just simply enlarge each authentication interval since it brings too much buffer space in each sensor.

As shown in Fig.6, we adapt a hierarchical broadcast authentication scheme. First we divide the whole lifetime into big time frames. Each frame has a 'frame key' and a pseudo-random function. Inside each 'frame', we further divide it into sub-intervals. We use μTESLA in each 'frame'. The sub-intervals have corresponding authentication keys and a common pseudo-random function. The high-level keys can generate low-level

keys.

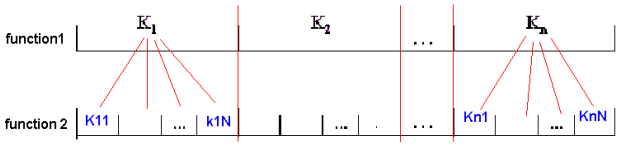

Fig.6

7. CONCLUSIONS

Security is the linchpin of good sensor network design. This paper analyzed security challenges in wireless sensor networks and summarized key issues that should be solved for achieving the WSN security. It also gave an overview of the current state of solutions on three key issues including the prevention of Denial-of-service detection, secure routing and key management service. We also summarized our integrated wireless security scheme that considered the specific routing characteristics of sensor networks: large-scale, dynamic topology and low-energy.

References:

[1] Akyildiz, I., Su, W., Sankarasubramaniam, Y., and Cayirci, E., "A Survey on Sensor Networks", *IEEE Communications Magazine*, August 2002.

[2] Balenson, D., et al, "Communications Security Architecture for Army Sensor Networks", NAI Labs T.R. #00-016, September 30, 2000.

[3] Carman, D., Kruus, P., Matt, B., "Constraints and Approaches for Distributed Sensor Network Security", NAI Labs T.R. #00-010, June 1, 2000.

[4] A. Perrig, R. Szewczyk, V. Wen, D. culler, and J. Tygar. "*SPINS: Security Protocols for Sensor Networks*." In Seventh Annual ACM International Conference on Mobile Computing and Networks(Mobicom 2001), Rome Italy, July 2001.

[5] S. Basagni, K. Herrin, D. Bruschi, and E. Rosti. "Secure pebblenets." In Proceedings of the 2001 ACM International Symposium on Mobile Ad Hoc Networking and Computing, pages 156-163. ACM Press, October 2001.

[6] Jeffery Undercoffer, Sasikanth Avancha, Anupam Joshi and John Pinkston, "Security for Sensor Networks," 2002 CADIP Research Symposium, http://www.csee.umbc.edu/cadip/2002Symposium/.

[7] N. Asokan and P. Ginzboorg, "Key Agreement in Ad Hoc Networks", Computer Communications, Volume 23, Pages 1627-1637

[8] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks", IEEE Networks, Volume 13, Issue 6 1999

[9] J. Kong, P. Zerfos, H. Luo, S. Lu and L. Zhang, "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks, IEEE ICNP 2001.

[10] C. Perkins, "Ad Hoc Networks", Addison-Wesley, Reading, MA, 2000.

[11] A. D. Wood and J. A. Stankovic. "*Denial of Service in Sensor Networks"*. IEEE Computer, October 2002, pp 54-62.

[12] C. Gehrmann. "BluetoothTM Security White Paper". White paper, Bluetooth SIG Security Expert Group, Apr 2002.

[13] Y. W. Law, S. Dulman, S. Etalle and P. Havinga. "Assessing Security-Critical Energy-Efficient Sensor Networks", Department of Computer Science, University of Twente, Technical Report TR-CTIT-02-18, Jul 2002.

[14] Y.-C. Hu, A. Perrig, and D. B. Johnson. Ariadne: "A Secure On-Demand Routing Protocol for Ad Hoc Networks." Technical Report TR01-383, Department of Computer Science, Rice University, 2001.

[15] Zheng Yan, (Networking Laboratory, Helsinki University of Technology), "Security in Ad Hoc Networks," available from http://citeseer.nj.nec.com/536945.html.

[16] Pietro Michiardi and Refik Molva, "Prevention of Denial of Service attacks and Selfishness in Mobile Ad Hoc Networks." Research Report N° RR-02-063, January 2002.

[17] T. Aura, P. Nikander, and J. Leiwo, "DOS-Resistant Authentication with Client Puzzles," *Proc. Security Protocols Workshop 2000*, Springer-Verlag, New York, 2000, pp. 170-177.

[18] S. Marti, T. Giuli, K. Lai, and M. Baker. "*Mitigating routing misbehavior in mobile ad hoc networks*. " In Proceedings of MOBICOM, 2000.

[19] P. Michiardi and R. Molva. "Core: A COllaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks." In *Communications and Multimedia Security Conference*, 2002.

[20] P. Michiardi and R. Molva. "Prevention of denial of service attacks and selfishness in mobile ad hoc networks". Research Report RR-02-063, Institut Eur´ecom, France, 2002.

[21] P. Michiardi and R. Molva. "Simulation-based analysis of security exposures in mobile ad hoc networks". In *European Wireless 2002: Next Generation Wireless Networks: Technologies, Protocols, Services and Applications, February 25-28, 2002, Florence, Italy*, 2002.

[22] L. Blazevic, L. Buttyan, S. Capkun, S. Giordano, J.-P. Hubaux, and J.-Y. Le Boudec. "Self-organization in mobile ad hoc networks: the approach of terminodes." *IEEE Communications Magazine*, 39(6):164–174, June 2001.

[23] L. Butty´an and J.-P. Hubaux. Nuglets: "A Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks." Technical Report DSC/2001/001, Department of Communication Systems, Swiss Federal Institute of Technology, 2001.

[24] S. Buchegger, J.-Y. Le Boudec. "*Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks*." In Proceedings of the 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing, Canary Islands, Spain, January 2002.

[25] S. Yi, P. Naldurg, and R. Kravets. "Security-aware ad hoc routing for wireless networks." In *Proceedings of the 2001 ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pages 299–302. ACM Press, 2001.

[26] R. Wattenhofer, L. Li, P. Bahl, and Y. M. Wang. "*Distributed topology control for power efficient operation in multihop wireless ad hoc networks*." In Proc. IEEE Infocom, 2001

[27] Haas, Z. & Pearlman, M., "*Determining the Optimal Configuration for the Zone Routing Protocol*." IEEE Journal on Selected Areas in Communications, Special issue on Wireless Ad Hoc Networks, June 1999.

[28] B. Awerbuch and D. Peleg, "Sparse Partitions," *Proceedings of the 31st Annual Symposium on Foundations of Computer Science*, 1990, pp. 503-513,

[29] D. J. Baker, A. Ephremides, and J. A. Flynn, "The Design and Simulation of a Mobile Radio Network with Distributed Control," *IEEE Journal on Selected Areas in Communications*, Vol. SAC-2, pp. 226-237, Jan. 1984.

[30] D. Peleg and E. Upfal, "A Trade-Off Between Space and Efficiency for Routing Tables," *Journal of the ACM*, Vol. 36, No. 3, pp. 510-530, July 1989.

[31] A. Menezes, P. van Oorschot and S. Vanstone, Handbook of Applied Cryptography, CRC Press 1997, ISBN 0849385237

[32] H. Luo and S. Lu, "Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks", Technical Report 200030, UCLA Computer Science Department 2000.

[33] H. Luo, P. Zerfos, J. Kong, S. Lu and L. Zhang, "Self-securing Ad Hoc Wireless Networks", IEEE ISCC 2002.

[34] Klas Fokine. "Key Management in Ad Hoc Networks. " (Master Thesis). Available from: http://www.ep.liu.se/exjobb/isy/2002/3322/.

[35] J. P. Hubaux, L. Buttyan, and S. Capkun. "The quest for security in mobile ad hoc networks." In *Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), Long Beach, CA, USA*, October 2001.

[36] EYES project, University of Twente, The Netherlands, "security in wireless sensor networks," please go to their project website: http://wwwes.cs.utwente.nl/24cqet/adhoc.html.

[37] Laurent Eschenauer and Virgil D. Gligor, "A Key-management scheme for distributed sensor networks," CCS'02, November, 2002, Washington DC, USA.

[38] L. Feeney. "A taxonomy for routing protocols in mobile ad hoc networks". Technical Report T99/07, Swedish Institute of Computer Science, October 1999.

[39] University of California, Santa Barbara. "Ad hoc On-Demand Distance Vector Routing". Home page. http://moment.cs.ucsb.edu/AODV/aodv.html.

[40] Rice University. Rice University Monarch Project: "Mobile Networking Architectures." Home page. http://www.monarch.cs.rice.edu.

[41] C. E. Perkins, editor. *Ad Hoc Networking*. Addison Wesley, 2001.

[42] D. W. Carman, B. J. Matt, and G. H. Cirincione, "Energy-Efficient And Low-Latency Key Management For Sensor Networks," (obtained through contacting the authors).

[43] S. Yi, P. Naldurg, and R. Kravets. "Security-aware ad hoc routing for wireless networks." In *Proceedings of the 2001 ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pages 299–302. ACM Press, 2001.

[44] E. Ayanoglu, I. Chih-Lin, R. Gitlin, and J. Mazo. Diversity coding for selfhealing and fault tolerant communication networks. *IEEE Transactions on Communications*, 41(11):1677–1688, November 1993.

[45] L. Blazevic, L. Buttyan, S. Capkun, S. Giordano, J.-P. Hubaux, and J.-Y. Le Boudec. "Self-organization in mobile ad hoc networks: the approach of terminodes. *IEEE Communications Magazine*, 39(6):164–174, June 2001.

[46] Y.-C. Hu, A. Perrig, and D. B. Johnson. "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks." Technical Report TR01-383, Department of Computer Science, Rice University, 2001.

[47] Matt, B., "A Preliminary Study of Identity-based, Group Key Establishment Protocols for Resource Constrained Battlefield Networks", Technical Report 02-034, Network Associates Laboratories, Sept. 2002.

[48] Jing Deng, Richard Han and Shivakant Mishra, "INSENS: Intrution-Tolerant Routing in Wireless Sensor networks," TR CU-CS-939-02, Dept of Computer Science, University of Colorado.

[49] Kimaya Sanzgiri, Bridget Dahill, Brian N. Levine, Clay Shields, and Elizabeth M. Belding-Royer. "A Secure Routing Protocol for Ad hoc Networks." To

appear in the International Conference on Network Protocols (ICNP), Paris, France, November 2002.
[50] Yih-Chun Hu, A. Perrig, and D. B. Johnson. "Ariadne: A secure on-demand routing protocol ," Mobicom'02, September, 2002, Atlanda, USA.
[51] L. Ramachandran et al., "Clustering Algorithms for Wireless *Ad Hoc* Networks", Proceedings of the fourth international workshop on Discrete algorithm and methods for mobile computing and communication, 2000, pages 54-63.
[52] Suman Banerjee and Samir Khuller, "A Clustering Scheme for Hierarchical Control in Multi-hop Wireless Networks," IEEE Infocom 2001.
[53] W.R. Heinzelman, A. Chandrakasan, H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," IEEE Proceedings of the Hawaii International Conference on System Sciences, January 2000, pp. 1–10.
[54] W.R. Heinzelman, J. Kulik, H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks," Proceedings of the ACM MobiCom'99, Seattle, Washington, 1999, pp. 174–185.
[55] K. Sohrabi, J. Gao, V. Ailawadhi, G.J. Pottie, "Protocols for self-organization of a wireless sensor network," IEEE Personal Communications, October 2000, pp. 16–27.
[56] N.M. Haller, "The S/KEY one-time password system", In ISOC, 1994
[57] Pietro,R.; Mancini,L.V.; Jajodia,S., "Secure selective exclusion in Ad-hoc Wireless Network", Security in Infomation Society: Visions and Perspectives (book), M. Adeep Ghonaimy, Mahmoud,T.El-Hadidi, Heba, K. Aslan,eds., Kluwer Academic Publishers, Boston, pp. 423-434, 2002.
[58] K. Zhang. "*Efficient protocols for signing routing messages*." In Proceedings of the Symposium on Network and Distributed Systems Security (NDSS '98), San Diego, California, March 1998.
[59] NAI Lab, http://www.nai.com/nai_labs/asp_set/crypto/crypt_senseit.asp.
[60] B. Awerbuch, D. Holmer, C. Nita-Rotaru and H. Rubens, "An On-Demand Secure Routing Protocol Resilent to Byzantine Failures," ACM Workshop on Wireless Security (WISE) 2002, pp. 21-30.
[61] S. Gar_nkel, \PGP: Pretty Good Privacy," O'Reilly & Associates Inc., USA, 1995.
[62] A. Abdul-Rahman, \The PGP Trust Model," EDI-Forum: the Journal of Electronic Commerce, 1997
[63] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.
[64] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Inform. Theory*, IT-22:644–654, November 1976.
[65] P. Papadimitratos, Z. Haas, "Secure Routing for Mobile Ad hoc Networks," Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002).
[66] D. Ganesan, R. Govindan, S. Shenker and D. Estrin, "Highly Resilient, Energy Efficient Multipath Routing in Wireless Sensor Networks," Mobile Computing and Communication Review (MC2R) Vol 1., No.2. 2002.
[67] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols". Technical Report TR01-384, Department of Computer Science, Rice University, June 2002.
[68] D. W. Carman, P. S. Kruus and B. J. Matt. "Constraints and Approaches for Distributed Sensor Network Security".Sept 1, 2000. NAI Labs Technical Report #00-010
[69] Stephen Carter and Alec Yasinsac, "Secure Position Aided Ad hoc Routing Protocol". Proceedings of the IASTED International Conference on Communications and Computer Networks (CCN02), Nov 3-4, 2002.
[70] Bridget Dahill, Brian Neil Levine, Elizabeth Royer, Clay Shields. "A Secure Routing Protocol for Ad Hoc Networks", In Proceedings of the 10 Conference on Network Protocols (ICNP), November 2002.
[71] Yih-Chun Hu, David B. Johnson, and Adrian Perrig. "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks." Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002), pp. 3-13, IEEE, Calicoon, NY, June 2002.
[72] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar. "SPINS: Security Protocols for Sensor Networks," in Wireless Networks Journal (WINE), September 2002.
[73] Laurent Eschenauer, Virgil D. Gligor. "A key-management scheme for distributed sensor networks." Conference on Computer and Communications Security". Proceedings of the 9th ACM conference on Computer and communications security 2002 , Washington, DC, USA
[74] Yee Wei Law, Sandro Etalle, Pieter H. Hartel, "Key Management with Group-Wise Pre-Deployed Keying and Secret Sharing Pre-Deployed Keying", EYES project (Europe), available through GOOGLE search engine.
[75] Donggang Liu and Peng Ning "Location-Based Pairwise Key Establishments for Relatively Static Sensor Networks." 2003 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN

'03) October 31, 2003 George W. Johnson Center at George Mason University, Fairfax, VA, USA.
[76] Wenliang Du and Jing Deng, " A Pairwise Key Pre-Distribution Scheme for Wireless Sensor Networks," Conference on Computer and Communications Security archive Proceedings of the 10th ACM conference on Computer and communication security table of contents Washington D.C., USA, Pages: 42 – 51, 2003.
[77] W. Heinzelman, ``Application-Specific Protocol Architectures for Wireless Networks," PhD Thesis, *Massachusetts Institute of Technology*, June 2000.
[78] Haas, Z.J., Pearlman, M.R., Samar, P., "The Zone Routing Protocol (ZRP) for Ad Hoc Networks," IETF Internet Draft, draft-ietf-manet-zone-zrp-04.txt, July 2002.
[79] Fei Hu, Sunil Kumar, "Wireless Sensor Networks for Mobile Telemedicine: QoS support", IEEE Transactions on Information Technology in Bioinformatics, (under final review), 2003.
[80] BLOM, R., "An optimal class of symmetric key generation systems." Advances in Cryptology: Proceedings of EUROCRYPT 84 (Thomas Beth, Norbert Cot, and Ingemar Ingemarsson, eds.), Lecture Notes in Computer Science, Springer-Verlag 209, 335ñ338, 1985.