Available online at www.sciencedirect.com
SCIENCE DIRECT®
Ad Hoc Networks 3 (2005) 69–89
Ad Hoc Networks
www.elsevier.com/locate/adhoc

Security considerations in ad hoc sensor networks

Fei Hu [a,*], Neeraj K. Sharma [b]

[a] Department of Computer Engineering, Rochester Institute of Technology, Rochester, NY 14623, USA
[b] Department of Electrical and Computer Engineering, Clarkson University, Potsdam, NY 13699, USA

Received 13 January 2003; received in revised form 1 August 2003; accepted 6 September 2003
Available online 26 November 2003

Abstract

In future smart environments, ad hoc sensor networks will play a key role in sensing, collecting, and disseminating information about environmental phenomena. As sensor networks come to be 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 has been placed on security. This paper analyzes security challenges in wireless sensor networks and summarizes key issues that need be solved for achieving security in an ad hoc network. 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.

Keywords: Ad hoc networks; Sensor networks; Security

1. Introduction

Advances in micro-electro-mechanical systems (MEMS) technology, wireless communications, and digital electronics have enabled many new opportunities such as ad hoc sensor networks (ASN) to monitor and control the physical world. ASN consist of a large number of cooperating nodes that have limited energy resources, computation ability and wireless communication range. Thus they need to be energy-efficient, scalable.

When they are deployed in hostile environments, they also need strong security services including confidentiality, integrity, and group-level authentication of sensor data and routing control traffic. Although significant progress has been shown in developing ASN in many aspects including topology management, routing algorithms, data link protocol and sensor data management (please refer to a comprehensive review on Wireless Sensor Networks in [1]), very little work is done on securing ASN. Research into authentication and confidentiality mechanisms designed specifically for ASN is needed.

There are already some proposals addressing security in *general ad hoc networks* [1] [7–9,12]. ASN

* Corresponding author.
E-mail addresses: fei.hu@ieee.org (F. Hu), sharman@clarkson.edu (N.K. Sharma).

[1] *General ad hoc network* can be defined as follows [10]: It 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.

1570-8705/$ - see front matter
doi:10.1016/j.adhoc.2003.09.009

can be considered as a special type of *ad hoc networks*, but ASN have some additional concerns (see follows) that limit the applicability of those traditional security measures.

1. *Very low power consumption*: Sensor nodes carry limited, generally irreplaceable, power sources [1]. Many *general ad hoc networks* aim to achieve high quality of service (QoS) provisions such as low latency and reserved bandwidth, while sensor network protocols must focus primarily on power conservation.
2. *Very limited local memory and calculation capacity*: Any security mechanisms for ASN cannot require each sensor node to store lots of long-sized keys or run very complex cryptology protocols. However, most research work on *general ad hoc network* s does not put saving power in the first goal to be achieved.
3. *Large number of communication nodes*: The number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in a *general ad hoc network*. Usually sensor nodes are densely deployed. Sensor nodes may not have global identification (ID) because of the large amount of overhead and large number of sensors.
4. *Easy node failure*: Sensor nodes may fail or be blocked due to lack of power or physical damage. The failure of sensor nodes should not affect the overall task of the sensor network. This is the reliability or fault tolerance issue. Fault tolerance is the ability to sustain sensor network functionalities without any interruption due to sensor node failures [1]. The dynamic nature of ASN topology is typically due to node failure or node insertion instead of node mobility since most ASN applications do not assume a highly mobile characteristic [1]. However, in *general ad hoc networks*, node mobility is a bigger concern than node failure.

The above constraints 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].

Security is a very important issue for ASN networks, especially for security-sensitive military applications. Security should be considered for some network functions such as packet forwarding, routing and network management, which are carried out by some or all of the available nodes in the ASN networks. Due to the basic differences from fixed networks and *general ad hoc networks*, security in the ASN should be re-examined and reconsidered.

This paper aims to give an overview of the current state of the ASN security, to analyze its requirements and to discuss its challenges and technologies. The rest of this paper is organized as follows: in Section 2, the goals, challenges and key issues for securing sensor networks are briefly presented. Sections 3–5 discuss each of those issues respectively. Finally, we make the conclusions in Section 6.

2. ASN security: goals and challenges

In this section, we identify the security challenges in ASN posed to the research communities, discuss the security problems in each networking layer, and finally state the three key issues to be addressed.

2.1. ASN network model

In this paper, we consider a general ASN network model that has the following features:

1. Large-scale (>1000 nodes): Typical covered area size can be a battlefield with over 500 soldiers (use sensors to keep track of soldiers), a community with a radius of 1000 m (use medical sensors for mobile telemedicine), or a forest (use sensors to monitor animal habitation); It has a moderate density to make the sensors establish multi-path communication links.
2. Mobility mode: Sensors may be attached to mobile objects and thus make the network topology frequently changed. Re-keying needs to be

performed periodically to adapt to the sensor removing, insertion, or death due to out of power. We assume random-walk mobility mode in this paper. In this paper, we do not consider a highly dynamic ASN but assume a fixed-to-walking speed (less than 5 m/s).
3. Communication mode: An ASN runs at unlicensed frequency band such as 916 MHz. This paper assumes typical wireless transmission distance among sensors to be around 20 m, which is practical for many civilian or military applications.
4. Those sensors can self-organize to a peer-to-peer ad hoc network. In the other hand, when a user wants to send a query/command to the ASN, one or more base stations can be used to interface the ASN to the user or outside network. The base stations have high power and can reach a large part of the ASN. But a sensor has very limited communication range and can only use multi-hop mode to relay data to a base station. In this paper, we assume that the base station may or may not be trustworthy. In other words, we require that the sensors are able to generate shared keys for each link.
5. The sensors are tiny, low battery-powered devices such as UC Berkeley 'smart dusts' [4]. Typical parameters are as follows: Memory: 10–30 K bytes; CPU: 8-bit, 4 MHz; Data speed: less than 10 Kbps. We assume the battery in each sensor is irreplaceable, which is a normal case in most low-cost ASN applications.
6. The sensors can be tamper-resistant [2] or not, which depends on the cost of each sensor.

In summary, our network model requires that the security scheme cannot be traditional public-key encryption schemes that need too much memory for the key storage (for instance, RSA [4] need 1024 bits for each variable). The ad hoc nature requires that key management should adapt to the link failure and node removing/insertion.

[2] Tamper-resistant: When an attacker breaks a sensor, the security information (such as keys) will become inaccessible or not useful.

2.2. Security goals

When dealing with security in ASN, one is faced with the problem of achieving some or all of the following goals:

1. *Availability*: This means that network assets are available to authorized parties when needed and ASN should ensure the survivability of network services despite denial-of-service (DoS) attacks, which could be launched at any layer of ASN. To ensure the availability of message protection, the sensor network should protect its resources (i.e., sensor nodes) from the unnecessary processing of key management messages in order to minimize energy consumption and extend the life of the network [2,8].
2. *Authenticity*: In ASN, authentication is necessary for many administrative tasks (e.g. network reprogramming or controlling sensor node duty cycle). At the same time, an adversary might easily inject messages, so the receiver needs to make sure that the data used in any decision-making process originates from a trusted source. *Data authentication* allows the receiver to verify that the data was really sent by the claimed sender. Stronger levels of authenticity (e.g. explicit key authentication) are provided by some key establishment protocols. However, most ASN scenarios do not require the extra "assurance", and can verify key delivery by using a system/application protocol [2,4].
3. *Confidentiality*: A confidential message is resistant to revealing its meaning to an eavesdropper. Even routing information in ASN needs to remain confidential, since it may be used to in a DoS attack. The standard solution to keep sensitive data secret is to encrypt the data with a secret key that only the intended receivers possess, hence achieving confidentiality. Confidentiality should be provided by keys with as small a scope as possible (i.e. fine key granularity) to discourage a single break from compromising a large portion of the sensor network. In other words, establishing unique keys between every pair of communicating sensor

nodes is preferable, in a security sense, to using a single network-wide key [2,3].

4. *Freshness*: This could mean *data freshness* and *key freshness*. Since all sensor networks provide some forms of time varying measurements, we must ensure each message is *fresh*. Data freshness implies that the data is recent, and it ensures that no adversary replayed old messages [4]. A key establishment process among the participants should guarantee that each shared key (session key) is fresh (i.e. has not been reused by one of the participants). This also means that a key used in one cryptographic association has not been used in another association [2]. Thus shared keys need to be changed over time (i.e. rekeying) since a key (long term or session key) may be compromised during pre-deployment or operational phases of a ASN.
5. *Data integrity*: Integrity measures ensure that the received data is not altered in transit by an adversary. The integrity service can be provided using cryptographic hash functions along with some form of encryption. When dealing with network security, the integrity service is often provided implicitly by the authentication service.
6. *Scalability and self-organization*: In contrast to *general ad hoc networks* that do not put scalability in the first priority, ASN cannot utilize a keying scheme that has poor scaling properties (either in terms of energy cost or latency) for establishing and maintaining a key for the ASN as a whole or for some large subset of nodes [2]. In general, the number of neighbors, and the distances or power required to send a messages with a particular error rate from one node to another will not be known in advance. As a consequence, the ASN nodes must be able to self-organize and select the appropriate keying mechanism for the situation [3].

2.3. Challenges

Challenge 1: There exists a conflicting interest between minimizing *resource* consumption of sensor nodes and maximizing security performance.

The *resource* in this context includes energy as well as computational resource like CPU cycles and memory. The capabilities and constraints of a sensor node will seriously influence the type of security mechanisms that can be hosted on a sensor node platform.

- *Energy* is perhaps the greatest constraint to sensor node capabilities. The extra power consumed by sensor nodes due to security is related to the processing required for security functions (e.g., encryption, decryption, signing data, verifying signatures), the energy required to transmit the security related data or overhead (e.g., initialization vectors needed for encryption/decryption), and the energy required to store security parameters in a secure manner (e.g., cryptographic key storage). 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].
- The *sleep patterns* of sensor nodes have serious impacts on the receiving of security related commands and key materials. In order to maintain cryptographic synchronization throughout the sensor network, it is essential that all nodes use the proper cryptographic material when communicating. Failure to maintain or update to the correct keys could isolate a sensor node from communications with the rest of the network.
- *Tamper protection* add costs to each node. When designing the sensor network security architecture, we must assume that one or more sensor nodes within the network may be compromised [3]. Due to the lack of tamper protection available to sensor nodes, a sufficiently capable adversary can extract compromising cryptographic information from a sensor node. Tamper detection technologies can provide indication that tampering has occurred but have limited value in long-term unattended operations.

Challenge 2: The ad hoc networking topology renders a ASN susceptible to link attacks ranging from passive eavesdropping to active interfering.

Unlike fixed hardwired networks with physical defense at firewalls and gateways, attacks on an ASN can come from all directions and target at any node. Damage can include leaking secret

Table 1
Security challenges from the ad hoc topology of ASN

No.	Items	Impacts
1	Node mobility	Since it is difficult to track down a particular mobile node in a large-scale sensor network, attacks from a compromised node are more dangerous and much harder to detect. All these indicate that any node must be prepared to operate in a mode that trusts no peer
2	Node adding/failure	New nodes may be added or current nodes may die, thus ASN has a dynamic routing structure. Frequent routing changes can mean that the intermediate nodes processing data for an end-to-end session can change. Also, since many security services will be provided on a hop-by-hop basis, cryptographic key establishment will occur with local neighbors in the routing topology. If the routing changes, the set of local neighbors may change and thus cryptographic key establishment may need to occur again
3	Large amounts of nodes	Considering a large number of nodes in typical ASN, it is not practical to adopt centralized security measures. Instead, distributed security algorithms should be adopted. Introducing any central entity into security solution may cause fatal attack on the entire network once the centralized entity is compromised. Generally, decision making in the ASN is decentralized and many security algorithms rely on the cooperation of all nodes or partial nodes. New type of attacks can be designed to break the cooperative algorithm
4	Limited pre-configuration	The nature of ad hoc networking requires limited pre-configuration in order to support a flexible and easily deployable network. This constraint limits the amount and type of cryptographic material that should be necessary to deploy a secure sensor network
5	Node inattention	The sensor nodes may be unattended for long periods of time. For example, remote reconnaissance missions behind enemy lines may not have any physical contact with friendly forces once deployed. Although they may be managed remotely, in general sensor nodes are not in physical contact with ground troops once deployed. This makes it impossible for physical detection of tampering (i.e., through tamper seals) and physical maintenance (e.g., battery replacement). Other maintenance functions are possible (e.g., software updates, key updates) but must be done remotely. The amount of time that a sensor is left unattended increases the likelihood that an adversary has compromised its key material [3]

information, interfering message and impersonating nodes. Any of which may compromise the ASN security goals. Table 1 shows the impacts on security design due to the ad hoc topology of ASN.

Challenge 3: The wireless communication characteristics of ASN render traditional wired-based security schemes impractical. Table 2 lists salient networking features of ASN and their corresponding impacts on security design.

2.4. Security problems in each networking protocol layer

Here we will investigate the security problems from the point of view of Open System Interconnect (OSI) model. Fig. 1 is the typical layered networking model of ASN. The layered network architecture can improve robustness by circumscribing layer interactions and interfaces. A clean division of layers may be sacrificed for performance in sensor networks, however, reducing robustness. Each layer is vulnerable to different DoS attacks. Some attacks can even crosscut multiple layers or exploit interactions between them.

2.4.1. Physical layer

A well-known attack on wireless communication, jamming, can interfere with the radio frequencies that a network's nodes are using. An

Table 2
Impacts of wireless communication characteristics of ASN

Wireless communication characteristics	Impacts on security design
Limited radio transmission range	The communications range of sensor nodes is limited in order to conserve energy. Thus those security mechanisms designed for Long-haul communications capabilities of greater than 1 km are impractical for ASN
Limited communication bandwidth	Wireless bandwidth is very limited for low-cost sensor nodes. Thus the data rate in ASN is typically less than 1k bit/s [1]. Packet sizes within the sensor network are relatively small, potentially as small as 30 bytes with header [3]. The packet size determines the percentage of overhead in a given message. Cryptographic services should adhere to packet size restrictions in order to limit the amount of overhead and thus reducing the transmission energy penalty associated with transmitting the extra bits
Unreliable wireless links	Packet-based routing of the sensor network is connectionless and thus inherently unreliable. Packets may get damaged due to channel errors or dropped at highly congested nodes. The result is lost or missing packets. But reliability is required for the distribution of key material and security critical commands
Unidirectional channels	Not all communications channels are bi-directional. In some cases, unidirectional channels may exist where a sensor node is only capable of transmitting or receiving data but not both. Sometimes the sensor node may receive data but will not transmit until the danger of detection has subsided. Environmental or adversarial jamming may also cause communications links to be unidirectional. Unidirection may impact the design of energy-efficient cryptographic key distribution protocols in which energy intensive processing is shared between parties. Instead, one party would assume the bulk of the computations

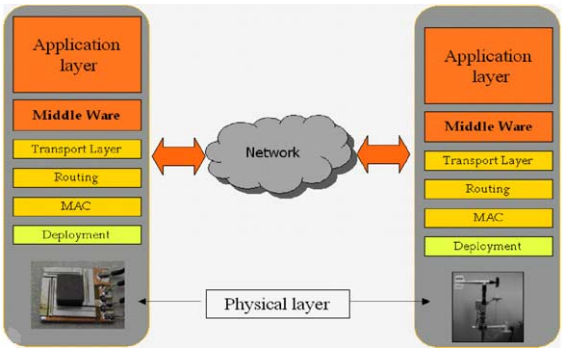

Fig. 1. Layered protocol stack of ASN.

adversary can disrupt the entire network with k randomly distributed jamming nodes, putting N nodes out of service, where k is much less than N. The standard defense against jamming involves various forms of *spread-spectrum* communication. Given that these abilities require greater design complexity and more power, low-cost, low-power sensor devices will likely be limited to single-frequency use [11].

Tampering is another type of physical attack in ASN. An attacker can damage or replace sensor and computation hardware or extract sensitive material such as cryptographic keys to gain unrestricted access to higher levels of communication. Tamper protection falls into two categories: active and passive [3]. Active tamper protection can involve the hardware circuits within the sensor node to protect sensitive data. Passive mechanisms include those that do not require energy and include technologies that protect a circuit or provide detection (e.g., protective coatings, tamper seals). Because these mechanisms may require extra circuitry that can add cost to a node and consume valuable energy, active mechanisms will not be typically found in sensor nodes. Instead, passive techniques are more indicative of sensor node technology.

2.4.2. Media access control layer

The media access control (MAC) layer provides channel arbitration for neighbor-to-neighbor communication. Typically, nodes have variable

control over their radiant RF energy allowing them to dynamically control the range of their communications and provide a lower probability of interception (LPI). Typically, this range is less than 100 m [3].

In the MAC layer, adversaries may only need to induce a collision in one octet of a transmission to disrupt an entire packet. A change in the data portion would cause a checksum mismatch at some other receiver. A corrupted ACK control message could induce costly exponential back-off in some MAC protocols. The amount of energy the attacker needs, beyond that required to listen for transmissions, is minute [11]. Large types of error-correcting codes can provide a flexible mechanism for tolerating variable levels of corruption in messages at any layer.

Security in MAC layer of ASN cannot simply borrow from other types of wireless networks. For example, Bluetooth provides data-link-level encryption [17], but it does not protect the network layers functions such as multi-hop routing [2].

2.4.3. Network routing layer

The sensor network utilizes a multi-hop bursty packet based network routing protocol to deliver data throughout the network. Attacks on the routing layer mainly include the following aspects (see Fig. 2) [13,14]:

- A sensor node without authentication creates *black holes* that aggressively sinks and drops messages that are routed through them;
- A node *floods* the whole ASN with illegitimate routing messages;

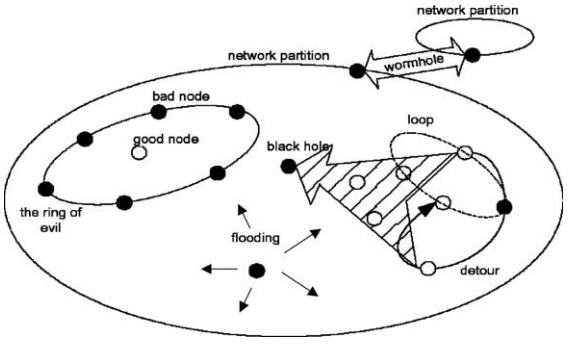

Fig. 2. Routing layer attacks in ASN.

- *Detours* and *loops* can be introduced to misdirect traffic, possibly through congested or energy-depleted routes;
- A *wormhole* is a covert channel between a pair of attacker nodes that creates a virtual vertex cut;
- A group of colluding malicious nodes may gang up and *hijack* a group of good nodes by refusing to route their packets, dropping their packets silently, or injecting bogus packets.

In ASN every node is potentially a router. This adds new vulnerabilities to the network layer problems experienced on the Internet. Routing protocols must be simple enough to scale up to large networks, yet robust enough to cope with failures that occur many hops away from a source.

2.4.4. Transport layer

The transport layer protocols can provide reliability and session control for sensor node applications. The majority of sensor network communications are bursty, packet-oriented communications that do not require the reliability of the transport layer. We generally assume that all sensor node communications are unreliable.

Generally speaking, if the data link layer and network layer are secure, then the transport layer can be sure that the packets it receives from the network layer are confidential, authenticated and original. What is left for the transport layer to do is the usual grunt work of flow control, packets reordering, error recovery and connection state management.

2.5. Major security issues

Based on the above analysis on the security goals, challenges and potential attacks in ASN, we can further summarize three key issues for achieving the security of ad hoc networks:

2.5.1. Key management in ASN

Confidentiality, integrity, and authentication services are critical to preventing an adversary from compromising the security of a ASN. Key management is likewise critical to establishing the keys necessary to provide this protection in ASN.

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 certificates for every node. The trusted CA is required to be online in many cases to support public key revocation and renewal. It is dangerous to set up a key management service using a single CA in a sensor network because single CA will be a vulnerable point of the network. If the CA is compromised, the security of the entire network is compromised.

2.5.2. Securing routing of ASN

There are two kinds of threats to ASN routing protocols [15]:

- *External attackers*: The attacks include injecting erroneous routing information, replaying old routing information, and distorting routing information. Using these methods, the attackers can successfully partition a network or introduce excessive traffic load into the network, therefore causing retransmission and ineffective routing. Using cryptographic schemes, such as encryption and digital signature can defend against the external attacks.
- *Internal compromised nodes*: They might send malicious routing information to other nodes. It is more difficult to detect such malicious information because compromised node can also generate valid signature.

There are routing protocols that cope well with the dynamic topology [26–30]. But those protocols offer little or no security features [8]. The 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 constraints.

2.5.3. Prevention of denial-of-service

Strictly speaking, although we usually use the term DoS to refer to an adversary's attempt to disrupt, subvert, or destroy a network, a DoS attack can be defined as 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 for ASN. 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 as follows: problem description, current research status and our suggested approach.

3. Key management in ASN

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.

Key management is an unsolved problem in ASN. Traditional Internet style key management protocols based on infrastructures using trusted third parties are impractical for large scale ASNs 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 two types of keying schemes in wireless sensor networks, i.e. *network-wide pre-deployed keying* and *node-specific pre-deployed keying*. [36] *Network-wide pre-deployed keying* equips every node in the network with the same key and equates the compromise of the single

system key with the compromise of the entire network. *Node-specific pre-deployed keying* assigns a unique key to every combination of communicating nodes. The security achieved by this scheme is optimal, however the storage requirement is unrealistic for low-cost sensor nodes.

Generally speaking, the problem of key management in ASN can be decomposed into the following six sub-problems:

- *Key pre-distribution*: To date, the only practical options for the distribution of keys to sensor nodes in ASN 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 pairwise 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 saving the key identifier of a key ring and associating sensor identifier with a trusted controller node.
- *Neighbor discovery*: In a certain wireless communication range, every node needs to discover its neighbors 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 ASN. 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*: 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. A path-key cannot be the one already used by the shared keys between neighbor nodes.
- *Isolating aberrant nodes*: An aberrant node is the 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 ASNs 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 challenging 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 make latency reduction an important factor.

3.2. State-of-the-art

Currently there are some key management schemes that can be *partially* used for securing ASN 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 types of sensor networks with different 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-efficient solution that is 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 extended to ASN environments. It uses a (k, n) threshold scheme to distribute the services of the CA 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 only for planned, long-term ad hoc networks instead of a ASN where sensor nodes can die in a short term due to lack of energy. 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 CA is first described by Luo and Lu in [32] and later analyzed by Luo et al. in [9,33]. 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 DoS 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 a 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 a crucial issue [45, p. 71]. In addition, in Pebblenets a key management server has to store not only 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 that must potentially be specialized nodes in the network, and the overhead in signing and verifying routing messages both in terms of computation and of communication.
- *Identity-based Group Keying Protocol*: Recently a series of group key transport protocols have been developed that provide requisite security properties using identity-based public key cryptography including ID-STAR-1 and ID-STAR-3 [47]. In each, the leader generates key material that is distributed to other group members using pairwise keys generated using identity-based cryptography rather than from certificates (see Fig. 3). In [42] the authors extend the use of identity-based group keying with the use of one-time identity-based keys to create

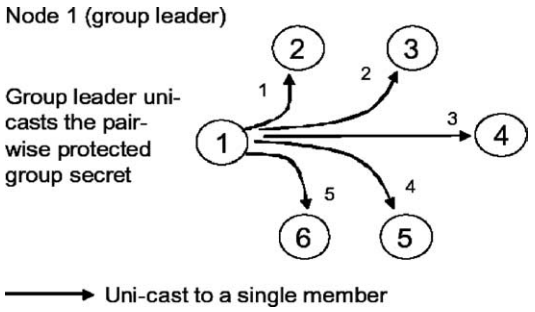

Fig. 3. ID-STAR.1 protocol.

a protocol that meets the security requirements of *Army sensor networks* while significantly reducing energy and latency costs versus existing certificate-based approaches by up to an order of magnitude.

- *Key-pool scheme*: A recent solution called selective key distribution scheme is proposed in [37] to save energy consumption in ASN. It relies on probabilistic key sharing among the nodes of a random graph and uses a simple shared-key discovery protocol for key distribution and re-keying. One drawback of this scheme is that some wireless links may not be keyed and thus a node may need to use a multi-link path to communicate with one of its neighbor nodes.

Table 3 compares the characteristics of the abovementioned key management protocols from the points of view of: (1) Level of its applicability to ASN; (2) Power saving; (3) Storage requirements; (4) Key distribution latency; (5) Collaboration ability (self-organization); and (6) Re-keying topology.

4. Secure routing in ASN

4.1. Problem description

There are many new routing protocols proposed for general ad hoc [38]. Among those routing protocols, the Ad hoc On-demand Distance Vector (AODV) protocol [39] and the dynamic source routing (DSR) protocol [40] have demonstrated very good performance [41]. There are also some schemes to secure ad hoc routing such as [46,49,56,57,67]. But most of those security schemes are not well suited to the typical ASN network model (refer to Section 2.1) due to their assumption of high power, large memory and small scale.

In Table 4 we list potential attacks in ASN routing protocols including AODV and DSR.

A more comprehensive classification on routing attacks is shown in Fig. 4.

All ASN routing security protocols must satisfy the following requirements in order to ensure that path discovery from source to destination functions correctly in the presence of malicious adversaries:

- Unauthorized nodes should be isolated during route discovery procedure.
- The network topology should not be revealed to adversaries.

Table 3
Comparison of key management protocols for ASN

Schemes	Applicable to ASN	Power consumption	Memory requirements	Key distribution latency	Self-organization	Re-keying topology
Hybrid	High	Depends	Depends	Average	Yes	Flat/Cluster
Threshold cryptography	Low	High	High	High	No	Flat
Certificate repository	Low	High	High	High	No	Flat
Fully Distributed Certificate Authority	Average	High	Average	Average	Yes	Flat
Pebblenets	High	Low	Low	Average	Yes	Cluster
Identity-based group Keying	High	Depends	Depends	Low	No	Cluster
Key-pool scheme	High	Average	Low	High	Yes	Flat

Table 4
Traditional ad hoc routing schemes have serious security limitations when used in ASN

Routing attacks	Meaning	AODV	DSR
Falsify route sequence numbers	AODV maintains routes by assigning monotonically increasing sequence numbers to each packet. When those numbers are changed, packets can be mistakenly considered to be misrouted or lost	Attack[a]	N/A
Modify hop count field of the header	AODV uses the hop count field in route discovery message to determine a shortest path. A malicious node can attract routes towards itself by resetting the hop count field to zero	Attack	N/A
Modify the source route field	DSR is a routing protocol which explicitly states routes in data packets. These routes lack any integrity checks and a simple DoS attack can be launched in DSR by altering the source routes in packet headers	N/A	Attack
Spoofing	Spoofing occurs when a node misrepresents its identity in the network, such as by altering its MAC or IP address in outgoing packets. Spoofing can produce loop paths	Attack	Attack
Falsify route error message	An attacker can issue route error messages to a normal node to indicate a broken link and thus misdirect the path	Attack	Attack
Corrupting routing table	An attacker can delete, alter or inject the information in routing tables so that the path is messed up	Defense	Attack

[a] *Attack* means this routing protocol (AODV or DSV) (shown in the table column) is vulnerable to this type of attack (shown in each table row). *N/A* means the routing protocol can prevent such an attack.

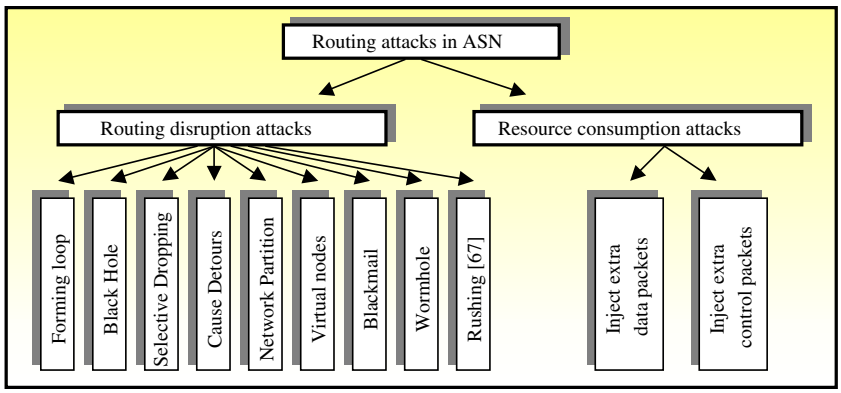

Fig. 4. Classification of ASN routing attacks.

- Paths should be immune to being misdirected (such as loop forming) from the shortest path by an attacker.
- Routing discovery messages cannot be spoofed.
- Identify fabricated routing message.

- Routing message cannot be altered in transmit by unauthenticated nodes.

To describe the ASN routing security problem, we can use the following symbols: *Denote A, B as* principals, such as communicating nodes; and K_{AB} and K_{BA} denote the secret MAC keys shared between A and B (one key for each direction of communication). $\mathrm{MAC}_{KAB}(M)$ denotes the computation of the *message authentication code* of message M with the key K_{AB}. We need to solve the following problems for securing ASN routing protocols:

1. An *authentication mechanism* with low computation and communication overhead is needed to prevent an attacker from performing a 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* 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 K_{AB} and K_{BA}, respectively, for message authentication in each direction. Route Discovery mechanisms should enable the target to verify the authenticity of the Route Requestor; They also need to authenticate data in route request messages and route reply messages through the using of K_{AB} and K_{BA}. 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* [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 the 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.
6. *Isolating malicious links*: A good secure routing mechanism needs to limit the route scope of damage caused by the (undetected) intruders through limiting flooding and using appropriate authentication mechanisms (see Fig. 5 [48]). In Fig. 5, the damage inflicted by a malicious node m is confined to a localized portion of the sensor network, i.e. nodes downstream from m and downstream from m's neighbors.

4.2. State-of-the-art

Little research work is done to secure ad hoc routing protocols. A security-enhanced version of AODV called Security-aware AODV (SAODV) is introduced in [43]. It is claimed that

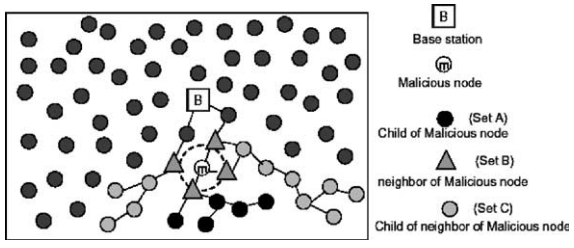

Fig. 5. Isolating malicious links in ASN.

SAODV achieves a satisfactory performance-overhead trade-off. However the fact that it is a metric-centric approach that relies on a user-defined, application-dependent parameter for evaluating trust level, does not solve the basis of the security problem. There are other approaches that taken advantage of *route redundancy* [44,45]. Besides security performance, energy consumption raises concern about the practicability of a particular protocol since energy is the most important factor in ASN.

For the problem of secure data forwarding, in [18] the authors propose two ideas to alleviate the detrimental effects of packet dropping: (i) detecting *misbehaving* nodes and reporting such events, and (ii) maintaining a set of metrics reflecting the past behavior of other nodes. Nevertheless, the plausibility of this solution could be questioned for three reasons:

- The possibility of falsely detecting misbehaving nodes could easily create a situation with many nodes falsely suspected for a long period of time.
- The metric construction may lead to a route choice that includes a suspected node, if, for example, the number of hops is relatively high, so that a low rating is "averaged out".
- The most important vulnerability is the proposed feedback itself; there is no way for the source, or any other node that receives a misbehavior report to validate its authenticity or correctness.

The above approaches to securing routing are most applicable to *general ad hoc* networks. However, their ideas can be *partially* used to secure ASN 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*: Security Protocols for Sensor Networks (SPINS) is one of the exceptions where routing is an application of a security framework [4]. SPINS scheme consists 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 used to provide authentication to data broadcasts. SPINS presents an architecture where the base station accesses nodes using source routing. The main idea of SPINS is to demonstrate the feasibility of security with very limited computing resources, by using symmetric cryptography alone, without emphasis on general applicability. The target wireless network is homogeneous and static. A central base station acts as the only point of trust, i.e. all nodes only trust the base station and themselves. As a result, the routing model that can be facilitated by SPINS is fairly limited: route discovery depends solely on the detection of authenticated beacons broadcast by the base station. Node-to-node communication necessitates authentication via the base station.
- *Pebblenets*: Pebblenet scheme [5] adopts cluster-based sensor network architecture as the foundation of data forwarding. It uses a global unique key and a hash function to generate session keys in each update round. One of the cluster-heads with higher power is chosen to become the key distribution center in each re-keying phase.
- *INSENS*: A recent solution called INtrusion-tolerant routing protocol for wireless SEnsor NetworkS (INSENS) for securing ASN routing is proposed in [48]. INSENS does not rely on detecting intrusions, but rather tolerates intrusions by bypassing the malicious nodes. 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. INSENS constructs forwarding tables at each node to facilitate communication between sensor nodes and a base station. It minimizes computation, communication, storage, and bandwidth requirements at the sensor nodes at the expense of increased computation, communication, storage, and bandwidth requirements at the base station.

4.3. Recommendations for securing ASN routing

Previous work on securing *ad hoc* routing that has serious resource constraints either due to its

using of public key cryptography [9,58,59] or significant computation and communication overhead [60], is not applicable to ASN. We suggest the following recommendations for securing ASN routing:

- Use *symmetric* cryptography instead of public/asymmetric key standard for *routing message authentication*and *routing discovery*.
  As the analysis in [4], 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 (e.g. RSA [63], Diffie-Hellman [64]), let alone perform operations with them. Keyed message authentication codes (MAC) [4] and one-way hash chains [48] are good solutions for securing ASN transmission.
- Tightly integrate *multi-path routing* algorithm with routing security system.
  A redundant multi-path routing algorithm such as [66] can provide fault tolerance and reliable data dissemination. Every node can have multiple paths to another node. A better choice is DPSP [65] that provides a fast multi-path routing algorithm based on a novel heuristic that picks a set of highly reliable paths. Since multi-path routing is useful to combat intrusions or malicious nodes, a good scheme is to tightly integrate it into a complete secure routing system [48].
- ASN Routing should be more like *Intrusion-tolerant* than *Intrusion-Detective*.
  It is difficulty to detect intrusions in a timely manner in sensor networks [48]. The values of some of the important parameters, such as normal usage and communication patterns, needed for (anomaly-based) intrusion detection are typically not known in advance in a sensor network, particularly in a critical scenario. Determining these values is time-consuming, and the presence of intruders can make it extremely difficult to determine these values. Thus, a better choice is to design a routing mechanism that is intrusion-*tolerant* rather than rely on traditional intrusion-detection techniques. This basically means that a malicious node can only compromise a very small number of nodes in its vicinity using attacks instead of causing widespread damage in the ASN.
- Use *localized trust model* instead of a centralized security management.
  Typically ASN is a type of dynamic ad hoc wireless network with large amount of nodes. Thus centralized trust management is difficult or expensive. Besides, a sensor node typically cares the trustworthiness of their immediate neighbors most due to the broadcast nature and the inherent local interactions of wireless transmissions. The node has to rely on its neighboring nodes for packet forwarding, routing and other network resource access. Therefore localized trust model like [32,61,62] is more appropriate for ASN routing protocol design. In localized trust model, a locally trusted entity is globally accepted and a locally distrusted entity is regarded untrustworthy anywhere.
- Reduce *routing overhead* when possible.
  Any ASN security protocol should have the reduction of communication cost as an important objective since sensors spend most of their energy in transmission instead of local procession. For example, we may allow the nodes to send substantially lighter routing information packets when the route Link State Updates (LSU) are redundant in respect of the previously exchanged information. The source node that sends the routing information to the other nodes can send a hash chain to the receiver instead of the complete routing updating message since hash functions are much faster compared to the digital signatures and other public-key methods [15].

5. Prevention of denial-of-service attacks in ASN

5.1. Problem description

In DoS attacks, the hacker's objective is to render target machines inaccessible by legitimate users. ASN 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, 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 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 ASN protocol layers [11]. Table 5 lists typical DoS attacks and the corresponding defense strategies.

Typical anti-DoS problem in sensor networks can be formulated as follows:

Define function f as any normal networking operations such as routing discovery and data packet forwarding. A node can become as a Requestor that issues the request of the execution of the function f to another node within its wireless communication range, called the Provider. The Requestor will monitor the result of the execution of f and, based on the outcome of the monitor result, it updates ratings relative to the monitored providers using the Reputation technique. Reputation [16] is usually defined as the amount of trust inspired by a particular member of a community in a specific setting or domain of interest. Members that have a good reputation, because they helpfully contribute to the community life, can use the resources while members with a bad reputation, because they refused to cooperate, are gradually excluded from the community. A node with a Reputation value larger than the Threshold is Trusted node while a node with a Reputation value below the Threshold is considered as a DoS attacker.

As shown in Fig. 6, suppose node c is a malicious node that produces DoS attacks when the sensor network tries to deliver packets from node a to node e. That is, node c does not cooperate to execute the function $f(\text{routing} : a \rightarrow e)$. Thus the anti-DoS mechanism needs to perform the following tasks:

- Quantitatively calculate the Reputation values of all nodes including node c. The Reputation

Table 5
Typical DoS attacks in ASN

DoS attacks	Meaning	Defense strategies
Radio interferences	In the Physical layer, an adversary sends randomly distributed jamming codes to disrupt normal radio transmission	• Use spread-spectrum • Go to sleeping mode periodically • Collaborate to reroute traffic
Physical tampering	An attacker captures and compromises the sensor nodes; He may also replace or extract useful information from nodes	• Make nodes tamper-resistant • Identify and exclude captured nodes
Denying channel	An attacker uses collision to damage the wireless channel and thus makes many packets useless	• Use error-correction code • Collision detection
Black holes	A malicious node in the route aggressively sinks and drops messages that are routed through them	• Multiple routing paths • Probe greedy nodes • Use redundancy
Misdirection	An attacker uses loop or detour to misdirect traffic	• Source authorization • Egress filtering
Flooding	A malicious node floods lots of messages to cause congestion and energy exhaustion	• Use client puzzles [17] • Limit the connections
Anti-synchronization	An attacker forges timing control messages to disrupt the synchronization between two nodes	• Authenticate packets
Critical attack	An attacker learns the critical resources such as cluster-heads and attacks them	• Hide important nodes

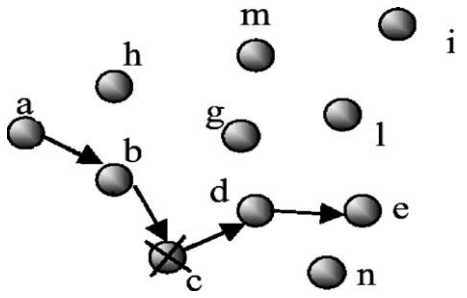

Fig. 6. Anti-DoS model.

should vary with time and be specific to a networking function f such as routing. We may denote the Reputation value of node c from the point of view of node b in time t as $\Re(t)|\times$ {objective_node $= c$, local_node $= b, f =$ routing}.

- Define a progressive factor $\delta|(t, t+\Delta)$ which should increase or decrease at a proper rate based on the matching level between the monitor results and the expected results

$$\Re_{\text{New}} = \Re_{\text{old}} \times \delta|(t, t+\Delta)$$

- Choose a reasonable Reputation threshold that differentiates between Trusted nodes and DoS attackers.
- Considering the thousands of nodes in ASN, the anti-DoS algorithm should be scalable and converge to a stable status quickly.
- The anti-DoS algorithm should integrate with different networking functions, i.e. different DoS attacks.

5.2. State-of-the-art

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.

It is difficult to establish trust and identity in large-scale, ad hoc sensor network deployments especially of ID-less nodes. Adding security *afterward* often fails in typical ASN systems. Thus *design-time* consideration of security offers the most effective defense against DoS attacks on availability.

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

- *Watchdog scheme*: 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]. Every node implements a watchdog that, operating in *promiscuous mode* (which consumes a great amount of energy), constantly monitors the packet forwarding activities of its neighbours, and a pathrater that rates the transmission reliability of all alternative routes to a particular destination node, according to the reports of the watchdog.
- *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. Rating Scheme striked a resonant chord on the importance of making "selfishness" pay. Selfishness is different from maliciousness in the sense that selfishness only aims at saving resources for the node itself by refusing to perform any function requested by the others, such as packet forwarding, and not at disrupting the flow of information in the network by intention.
- *Virtual currency*: This scheme introduces a type of 'selfish' nodes that are called *nuglets* [22,23]. To insulate a node's nuglets from illegal manipulation, a tamper-resistant *security module* storing all the relevant IDs, nuglet counter and cryptographic materials (but not the code) is compulsory. Two different models are used in this scheme: the Packet Purse Model and the Packet Trade Model. In the Packet Purse Model each packet is loaded with nuglets by the source and each forwarding host takes out nuglets for its forwarding service. The advantage of this approach is that it discourages users from flooding the network. In the Packet Trade Model each packet is traded for nuglets by the intermediate nodes: each intermediate node

Table 6
Disadvantages of current schemes when used in ASN for the prevention of DoS

Schemes	Disadvantages
Watchdog	• Only practical for source routing protocols instead of any general routing protocols • Collusion between malicious nodes remains an unsolved problem • Its assumption of the *promiscuous* mode of the wireless interface is not always true (as reckoned by the authors)
Rating	• The difficulty of this scheme lies in how an evaluating node is able to evaluate the result of a function executed by the evaluated node • Depending on the function executed, the evaluated node may be able to cheat easily • The result of the function may require significant overhead to be communicated to the evaluating node • If the requested function is simply forwarding packets, then the scheme faces similar difficulties faced by the watchdog mechanism
Virtual currency	• The cross-certification architecture calls for public key cryptography, which exerts a high demand on computing resources • The amount of overhead is a concern • Since the packet generation is not charged, malicious flooding of the network cannot be prevented • In its Packet Purse Model, the intermediate nodes are able to take out more nuglets than they are supposed to
Route DoS prevention	• Misbehaving nodes are not prevented from distributing bogus information on other nodes' behavior: the evaluation of a node behavior could then be erroneous and legitimate nodes can be classified as misbehaving nodes

buys the packet from the previous node on the path. Thus, the destination has to pay for the packet. The direct advantage of this approach is that the source does not need to know how many nuglets need to be loaded into the packet.

- *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. However, the mechanism they propose suffers from a DoS attack performed using the security mechanism itself. Indeed, misbehaving nodes are not prevented from distributing bogus information on other nodes' behavior: the evaluation of a node behavior could then be erroneous and legitimate nodes can be classified as misbehaving nodes. 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.

The above schemes were proposed to overcome DoS attacks in *general ad hoc net*works and were inadequate when applied in ASN due to their disadvantages [13,16] (see Table 6).

6. Conclusions

Security is the linchpin of good sensor network design. This paper reviewed three major issues in securing ASN and also proposed our technical approaches for solving those problems:

1. *Key Management*: It is an unsolved problem in ASN due to the limited resource including memory space and power capacity in each sensor node and the high scalability requirements of ASN. Our conclusion is that key management should adopt local-updated and global distributed algorithm and should be combined with topology management. Thus we proposed a multi-layer self-organization networking architecture that can efficiently carry out periodical re-keying algorithm.

2. *Secure Routing*: Most ASN routing protocols do not have a built-in security mechanism. Traditional approaches for securing *general ad hoc networks* are not applicable to ASN since those schemes do not put saving energy consumption as the first concern. Our recommendation is that a good secure routing scheme should tightly integrate the multi-path protocol into a complete secure routing system since multi-path routing is useful to combat intrusions or malicious nodes.
3. *Prevention of denial-of-service attacks*: DoS attacks can happen in each layer of ASN protocol suite. A necessary operation to overcome DoS attacks is to identify and circumvent the misbehaving nodes. The concept of *Reputation* is a good measure for identifying misbehaving nodes.

Our future research tasks consist of the following aspects:

- Finding more energy-efficient re-keying sensor networking architecture. Right now we simply finds *the largest* cluster available, whereas a smaller cluster may provide a greater reduction in energy consumption depending on the relative positions of the cluster members [51–55]. In addition, the overlapping between clusters has not been determined.
- Re-keying for *high-density* sensor networks. Multi-hop re-keys appears to be less energy-efficient. However, for densely populated sensor networks, the multi-hop keying may be more effective.
- *Combination of routing and security protocols*. Despite the additional complexity of integrating routing and key establishment protocols, there may be significant advantages in combining some aspects of these protocols. For instance, some key establishment protection is necessary to protect routing determination protocols. However, some multi-hop key establishment protocols require routing to already be determined. Integrating portions of both protocols together may provide energy reductions not possible with these functions separated [2].
- Other security services besides key management. Key management is but one of the many security services that must be supported by the distributed sensor network. It is necessary to examine other security services, such as integrity, authentication, and non-repudiation, to determine efficient and secure methods of providing these services.

References

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, A survey on sensor networks, IEEE Commun. Mag. 40 (8) (2002) 102–114.
[2] D. Balenson et al., Communications security architecture for army sensor networks, NAI Labs T.R. #00-016, 30 September 2000.
[3] D. Carman, P. Kruus, B. Matt, Constraints and approaches for distributed sensor network security, NAI Labs T.R. #00-010, 1 June 2000.
[4] A. Perrig, R. Szewczyk, V. Wen, D. culler, 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, E. Rosti, Secure pebblenets, in: Proceedings of the 2001 ACM International Symposium on Mobile Ad Hoc Networking and Computing, ACM Press, New York, 2001, pp. 156–163.
[6] J. Undercoffer, S. Avancha, A. Joshi, J. Pinkston, Security for sensor networks, 2002 CADIP Research Symposium. Available from <http://www.csee.umbc.edu/cadip/2002Symposium/>.
[7] N. Asokan, P. Ginzboorg, Key agreement in ad hoc networks, Comp. Commun. 23 (2000) 1627–1637.
[8] L. Zhou, Z.J. Haas, Securing ad hoc networks, IEEE Network 13 (6) (1999) 24–30.
[9] J. Kong, P. Zerfos, H. Luo, S. Lu, 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, J.A. Stankovic, Denial of service in sensor networks, IEEE Comp. 35 (10) (2002) 54–62.
[12] C. Gehrmann, BluetoothTM Security White Paper, White paper, Bluetooth SIG Security Expert Group, April 2002.
[13] Y.W. Law, S. Dulman, S. Etalle, P. Havinga, Assessing security-critical energy-efficient sensor networks, Department of Computer Science, University of Twente, Technical Report TR-CTIT-02-18, July 2002.
[14] A. Perrig, H. Chan, D. Song, Random key predistribution schemes for sensor networks, IEEE Symposium on Security and Privacy, 2003.

[15] Z. Yan, Security in ad hoc networks, Networking Laboratory, Helsinki University of Technology. Available from <http://citeseer.nj.nec.com/536945.html>.
[16] P. Michiardi, R. Molva, Prevention of denial of service attacks and selfishness in mobile ad hoc networks, Research Report No RR-02-063, January 2002.
[17] T. Aura, P. Nikander, J. Leiwo, DOS-resistant authentication with client puzzles, in: Proceedings of Security Protocols Workshop 2000, Springer, New York, 2000, pp. 170–177.
[18] S. Marti, T. Giuli, K. Lai, M. Baker, Mitigating routing misbehavior in mobile ad hoc networks, in: Proceedings of MOBICOM, 2000.
[19] P. Michiardi, 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, R. Molva, Prevention of denial of service attacks and selfishness in mobile ad hoc networks, Research Report RR-02-063, Institut Eurécom, France, 2002.
[21] P. Michiardi, 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, Florence, Italy, 25–28 February 2002.
[22] L. Blazevic, L. Buttyan, S. Capkun, S. Giordano, J.-P. Hubaux, J.-Y. Le Boudec, Self-organization in mobile ad hoc networks: the approach of terminodes, IEEE Commun. Mag. 39 (6) (2001) 164–174.
[23] L. Buttyáan, 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, 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, ACM Press, New York, 2001, pp. 299–302.
[26] R. Wattenhofer, L. Li, P. Bahl, Y.M. Wang, Distributed topology control for power efficient operation in multihop wireless ad hoc networks, in: Proceedings of IEEE Infocom, 2001.
[27] M. Pearlman, Z. Haas, Determining the optimal configuration for the zone routing protocol, IEEE J. Select. Area. Commun., Special issue on Wireless Ad Hoc Networks 17 (8) (1999) 1395–1414.
[28] B. Awerbuch, D. Peleg, Sparse partitions, in: Proceedings of the 31st Annual Symposium on Foundations of Computer Science, 1990, pp. 503–513.
[29] D.J. Baker, A. Ephremides, J.A. Flynn, The design and simulation of a mobile radio network with distributed control, IEEE J. Select. Area. Commun. SAC-2 (1) (1984) 226–237.
[30] D. Peleg, E. Upfal, A trade-off between space and efficiency for routing tables, J. ACM 36 (3) (1989) 510–530, July.
[31] A. Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, FL, 1997.
[32] H. Luo, 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, L. Zhang, Self-securing ad hoc wireless networks, IEEE ISCC, 2002.
[34] K. 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, 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, Security in wireless sensor networks, University of Twente, The Netherlands. Available from <http://wwwes.cs.utwente.nl/24cqet/adhoc.html>.
[37] L. Eschenauer, V.D. Gligor, A key-management scheme for distributed sensor networks, CCS'02, Washington, DC, USA, November 2002.
[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. Available from <http://moment.cs.ucsb.edu/AODV/aodv.html>.
[40] Rice University, Rice University Monarch Project: Mobile Networking Architectures. Home page. Available from <http://www.monarch.cs.rice.edu>.
[41] C.E. Perkins (Ed.), Ad Hoc Networking, Addison-Wesley, Reading, MA, 2001.
[42] D.W. Carman, B.J. Matt, G.H. Cirincione, Energy-efficient and low-latency key management for sensor networks, obtained through contacting the authors.
[43] A. Perrig, Y.-C. Hu, D. Johnson, Efficient security mechanisms for routing protocols, in: Proceedings of the 10th Annual Network and Distributed System Security Symposium (NDSS 2003).
[44] E. Ayanoglu, I. Chih-Lin, R. Gitlin, J. Mazo, Diversity coding for selfhealing and fault tolerant communication networks, IEEE Trans. Commun. 41 (11) (1993) 1677–1688.
[45] L. Blazevic, L. Buttyan, S. Capkun, S. Giordano, J.-P. Hubaux,, J.-Y. Le Boudec, Self-organization in mobile ad hoc networks: the approach of terminodes, IEEE Commun. Mag. 39 (6) (2001) 164–174.
[46] Y.-C. Hu, A. Perrig, 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] B. Matt, A preliminary study of identity-based, group key establishment protocols for resource constrained battlefield networks, Technical Report 02-034, Network Associates Laboratories, September 2002.
[48] J. Deng, R. Han, S. Mishra, INSENS: Intrution-tolerant routing in wireless sensor networks, TR CU-CS-939-02, Dept of Computer Science, University of Colorado.
[49] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding-Royer, A secure routing protocol for ad hoc networks, in: International Conference on Network Protocols (ICNP), Paris, France, November 2002, in press.
[50] A. Perrig, R. Canetti et al., The TESLA Broadcast Authentication Proctocol. Available from <http://www.ece.cmu.edu/~adrian/publications.html>.
[51] L. Ramachandran et al., Clustering algorithms for wireless ad hoc networks, in: Proceedings of the Fourth International Workshop on Discrete Algorithm and Methods for Mobile Computing and Communication, 2000, pp. 54–63.
[52] S. Banerjee, S. 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, in: 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, in: Proceedings of the ACM MobiCom'99, Seattle, WA, 1999, pp. 174–185.
[55] K. Sohrabi, J. Gao, V. Ailawadhi, G.J. Pottie, Protocols for self-organization of a wireless sensor network, IEEE Person. Commun. 7 (5) (2000) 16–27.
[56] N.M. Haller, The S/KEY one-time password system, in: ISOC, 1994.
[57] R. Pietro, L.V. Mancini, S. Jajodia, Secure selective exclusion in ad-hoc wireless network, in: M.A. Ghonaimy, T. Mahmoud, E.-H. Heba, K. Aslan (Eds.), Security in Infomation Society: Visions and Perspectives, Kluwer Academic Publishers, Boston, 2002, pp. 423–434.
[58] K. Zhang, Efficient protocols for signing routing messages, in: Proceedings of the Symposium on Network and Distributed Systems Security (NDSS '98), San Diego, CA, March 1998.
[59] NAI Lab. Available from <http://www.nai.com/nai_labs/asp_set/crypto/crypt_senseit.asp>.
[60] B. Awerbuch, D. Holmer, C. Nita-Rotaru, H. Rubens, An on-demand secure routing protocol resilent to byzantine failures, in: ACM Workshop on Wireless Security (WISE), 2002, pp. 21–30.
[61] S. Garnkel, PGP: Pretty Good Privacy, O'Reilly, Sebastopol, CA, 1995.
[62] A. Abdul-Rahman, The PGP Trust Model, EDI-Forum: J. Electron. Commerce, 1997.
[63] R.L. Rivest, A. Shamir, L.M. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM 21 (2) (1978) 120–126.
[64] W. Diffie, M.E. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory IT-22 (6) (1976) 644–654.
[65] P. Papadimitratos, Z. Haas, Secure routing for mobile ad hoc networks, in: Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002).
[66] D. Ganesan, R. Govindan, S. Shenker, D. Estrin, Highly resilient, energy efficient multipath routing in wireless sensor networks, Mobile Comput. Commun. Rev. (MC2R) 1 (2) (2002).
[67] Y.-C. Hu, A. Perrig, D.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.

Fei Hu is currently working as an assistant professor in Department of Computer Engineering, Rochester Institute of Technology in Rochester, New York. He obtained his Ph.D. degree in 2002 in Electrical and Computer Engineering at Clarkson University, Potsdam, New York. He received Master degree in Telecommunication Engineering from Shanghai Tiedao University of China in 1996. His research interests include high-speed computer networks, wireless & mobile computing, Internet and ATM.

Neeraj K. Sharma is currently a system engineer at Intel Corporation. From 1999–2000 he was an associate professor with the Department of Electrical and Computer Engineering, Clarkson University, Potsdam, NY. From 1993–1998 he was a faculty with the Department of Computer Science and Computer Engineering, La Trobe University, Melbourne, Australia. He received his Ph.D. and MSEE from the University of Akron, Akron, Ohio and BSEE from University of South Alabama, Mobile, Alabama all in Electrical Engineering. His research interests include fault-tolerant system design, and performance and reliability analysis of computer systems and networks.