Two Tier Secure Routing Protocol for Heterogeneous Sensor Networks

Xiaojiang Du, *Member, IEEE,* Mohsen Guizani, *Senior Member, IEEE,* Yang Xiao, *Senior Member, IEEE,* and Hsiao-Hwa Chen, *Senior Member, IEEE*

***Abstract*— Research on sensor network routing focused on efficiency and effectiveness of data dissemination. Few of them considered security issues during the design time of a routing protocol. Furthermore, previous research on sensor networks mainly considered homogeneous sensor networks where all sensor nodes have the same capabilities. It has been shown that homogeneous ad hoc networks have poor fundamental performance limits and scalability. To achieve better performance, we adopt a Heterogeneous Sensor Network (HSN) model. In this paper, we present a secure and efficient routing protocol for HSNs - Two Tier Secure Routing (TTSR). TTSR takes advantage of powerful high-end sensors in an HSN. Our security analysis demonstrates that TTSR can defend typical attacks on sensor routing. Our performance evaluation shows that TTSR has higher delivery ratio, lower end-to-end delay and energy consumption than a popular sensor network routing protocol.**

***Index Terms*— Heterogeneous sensor network, routing, secure routing, security.**

I. Introduction

WIRELESS sensor networks have many applications, such as military, homeland security, environment, agriculture, manufacturing, and so on. Routing is an essential operation in sensor networks. A number of routing protocols have been proposed for sensor networks, such as Directed Diffusion [1] and LEACH [2]. However, most routing protocols did not consider security issues during the protocol design phase. Providing security in sensor networks is challenging. Compared with conventional desktop computers, severe challenges exist since sensor nodes have limited capabilities in processing, storage space, bandwidth, and energy.

Most existing work in sensor networks considered routing protocols and security schemes (such as key management) separately. Few researchers consider security during the design phase of a routing protocol. Since most existing routing protocols have not been designed with security as a goal, they are vulnerable to many attacks. However, it is nontrivial to fix the problem since it is unlikely that a sensor network routing protocol can be made secure by incorporating security mechanisms after the design has completed [3]. To achieve secure routing in sensor networks, security should be considered during the design time of a routing protocol.

Most existing work on sensor networks considers homogeneous sensor networks where all sensor nodes are modeled to have the same capabilities in communications, computation, memory storage, energy supply, reliability and other aspects. However, a homogeneous ad hoc network has poor fundamental limits and performance. Its performance bottleneck has been demonstrated via theoretical analysis [4], simulation experiments and testbed measurements [5]. We notice that more and more recently deployed sensor networks follow heterogeneous designs, incorporating a mixture of sensor nodes with different capabilities. For example, a sensor network in [6] includes small MICA2 sensors (manufactured by Crossbow Technology [7]) as well as more powerful Personal Digital Assistants. Several recent papers (e.g., [8]–[12]) have studied Heterogeneous Sensor Networks (HSNs). These literatures showed that HSNs can significantly improve sensor network performance. In the past several years, much work (e.g., [13]–[17]) has been done on security issues in homogeneous sensor networks.

In this paper, we present a secure and efficient routing protocol for HSNs. The main contributions of this paper include: 1) security schemes specifically for HSNs by utilizing powerful high-end sensors; 2) a novel secure routing protocol for HSNs by considering security during the design phase of the routing protocol; and 3) the proposed secure routing protocol achieves better routing performance than Directed Diffusion [1].

The rest of the paper is organized as follows. We describe the HSN model in Section II, and present the Two Tier Secure Routing (TTSR) protocol in Section III. In Section IV, we mathematically show that the probability of having at least one high-end sensor in a certain area is high when there are sufficient high-end sensors. We present the security analysis and routing performance evaluation of TTSR in Sections V and VI, respectively. Finally, we conclude the paper in Section VII.

II. The HSN Model

Our current HSN model consists of two physically different types of sensor nodes: a small number of powerful High-end sensors (H-sensors) and a large number of Low-end sensors (L-sensors). We adopt a typical assumption about

Manuscript received February 6, 2006; revised July 27, 2006; accepted September 25, 2006. The associate editor coordinating the review of this paper and approving it for publication was X. Zhang.

X. Du is with the Dept. of Computer Science, North Dakota State Univ., Fargo, ND 58105 USA (e-mail: dxj@ieee.org).

M. Guizani is with the Dept. of Computer Science, Western Michigan Univ., Kalamazoo, MI 49008 USA (e-mail: mguizani@ieee.org).

Y. Xiao is with the Dept. of Computer Science, Univ. of Alabama, Tuscaloosa, AL 35487 USA (e-mail: yangxiao@ieee.org).

H.-H. Chen is with the Department of Engineering Science, National Cheng Kung University, Taiwan (e-mail: hshwchen@ieee.org).

Digital Object Identifier 10.1109/TWC.2007.06095.

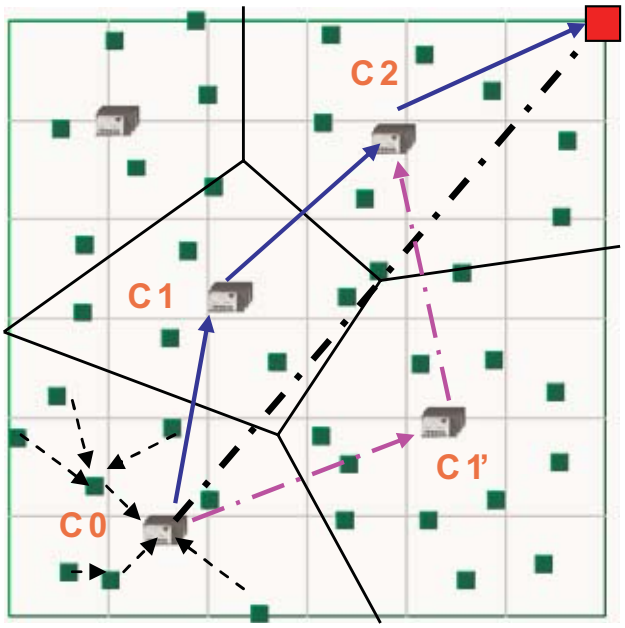

Fig. 1. Inter-cluster routing in an HSN.

sensor distribution and assume that both L-sensors and H-sensors are uniformly and randomly distributed in the field. After sensor deployment, clusters are formed in an HSN. It is natural to let powerful H-sensors serve as cluster heads and form clusters around them. All the H-sensors form a backbone in the network. An example of the cluster formation is shown in Fig. 1, where the small squares are L-sensors, large rectangles are H-sensors, and the large square at the top-right corner is the Base Station (BS). Powerful H-sensors have more energy supply, longer transmission range, higher data rate than L-sensors, and they provide many advantages for designing better protocols, algorithms, and secure schemes in sensor networks. We designed an efficient and robust cluster formation scheme for HSNs in [11]. Because of page limit, we will not describe the scheme here. We present assumptions of HSNs below.

1) Due to cost constraints, L-sensors are NOT equipped with tamper-resistant hardware. Assume that if an adversary compromises an L-sensor, she can extract all key material, data, and code stored on that node.
2) Each L-sensor (and H-sensor) is static and aware of its own location. Sensors may use a secure location discovery service (e.g., [17]) to estimate their locations, and no GPS receiver is required at each node.
3) H-sensors are equipped with tamper-resistant hardware. The number of H-sensors in an HSN is relatively small (e.g., 20 H-sensors and 1,000 L-sensors in an HSN). Hence, the total cost of tamper-resistant hardware in an HSN is small. Thus, it is reasonable to assume that powerful H-sensors have tamper-resistant hardware.
4) The base station is well protected and trustable.

III. Two Tier Secure Routing

The primary functionality of a wireless sensor network is to sense the environment and transmit the acquired information to the BS for further processing. Thus, routing is an essential operation in sensor networks. Typical sensor nodes are small, unreliable devices and are prone to failures. A routing protocol should be robust to sensor failures and be able to find new paths when nodes fail. Security requirement adds new challenges to routing. Recent literatures (e.g., [8]–[12] and [16]) have shown that HSNs can significantly improve performance and security of sensor networks.

In an HSN, the BS, H-sensors and L-sensors form hierarchical network architecture. The basic idea of routing in HSNs is to let each L-sensor sends data to its cluster head (an H-sensor). An H-sensor may aggregate data from multiple L-sensors and remove redundant data, and then send compressed data to the BS via the H-sensor backbone. Transmissions in the backbone have longer range and may use a different frequency than transmissions among L-sensors. Based on the above two-layer communication architecture, we designed a secure and efficient routing protocol for HSNs, and it is referred to as Two-Tier Secure Routing (TTSR) protocol. TTSR consists of two parts: secure routing within a cluster (among L-sensors), and secure routing across clusters (among H-sensors). We discuss each part of TTSR below.

A. Secure Intra-Cluster Routing

Routing within a cluster (from an L-sensor to its cluster head) is referred to as intra-cluster routing. After key setup by an HSN key management scheme (e.g., the one in [16]), each L-sensor has one shared-key with every neighbor L-sensor. Consider two neighbor L-sensors u and v, and denote their shared-key as K_s. Assume node ID $u < v$. L-sensors u and v need to perform the following two-way handshake before exchanging any data: 1) The L-sensor with smaller node ID - u sends a *challenge message* to v: $\{u, N_0\}K_s + MAC(K_s, *)$, where nonce N_0 is a one-time random number generated by u, and $MAC(K_s, *)$ denotes the Message Authentication Code (MAC) generated from message using key K_s. 2) Then v replies with a *response message* to u: $\{v, K_{u,v}, K_v^b, N_0 + 1\}K_s + MAC(K_{u,v}, *)$, where $K_{u,v}$ and K_v^b are keys generated by v. $K_{u,v}$ is the new pairwise shared-key used for the later communication between u and v, and K_v^b is a broadcast key for v.

The above two-way handshake can avoid (or defend against) the unidirectional link problem (or attack) [15]. For example, if u is a more powerful node (such as a laptop with a longer transmission range) than v, then u can send a packet to v directly, but v can not send a packet to u in one-hop. However, node v still thinks that u is a one-hop neighbor, and various problems may arise.

Each L-sensor sends packets to its cluster head (an H-sensor). We use the bottom-left cluster in Fig. 1 to illustrate the intra-cluster routing scheme. The basic idea is to let all L-sensors in a cluster form a tree rooted at the cluster head (denoted as H). It has been shown in [18] that: 1) If complete data fusion is conducted at intermediate nodes, (i.e., two k-bit packets come in, and one k-bit packet goes out after data fusion), then a minimum spanning tree (MST) consumes the least total energy in the cluster. 2) If there is no data fusion within the cluster, then a shortest-path tree (SPT) consumes

the least total energy. 3) For partial fusion, it is a NP-complete problem of finding the tree that consumes the least total energy. If data from nearby sensors are highly correlated, then an MST can be adopted to approximate the least energy consumption case. A centralized algorithm can be used by the cluster head to construct an MST. Each L-sensor sends its location information to the cluster head H during the key setup phase. A greedy geographic routing protocol (e.g., [19]) is used to forward an L-sensor's location information to H. During cluster formation, the location of H is broadcasted to all L-sensors in the cluster. Then H runs a centralized MST algorithm (e.g., the Kruskal's algorithm [20]) to construct the MST, and disseminates the MST structure information to L-sensors, i.e., informing each L-sensor which node its parent is. If there is few or no data fusion among L-sensors, an SPT should be used to approximate the least total energy consumption. Similarly, the cluster head H can construct an SPT by using a centralized algorithm and the locations of L-sensors.

Since L-sensors are small, unreliable devices and may fail over time, and therefore, robust and self-healing routing protocols are critical for routing among L-sensors. In the above route setup, each L-sensor may record two or more parent nodes. One parent node serves as the primary parent, and other parent nodes serve as backup parents. If the primary parent node fails, an L-sensor can use a backup parent for data forwarding. Each L-sensor records one or more backup cluster heads during cluster formation [11]. When a cluster head fails, L-sensors in the cluster send their packets to a backup cluster head.

After the routing tree (an MST or an SPT) is constructed, the following secure data forwarding scheme is used by L-sensors. Assume that L-sensor u sends data packets to its parent v.

1) $u \rightarrow v$: $packet\_ID + \{Data\}K_{u,v} + MAC(K_{u,v}, *)$, where the data is encrypted with the shared-key $K_{u,v}$, and $packet\_ID$ (not encrypted) is a local ID assigned by the sender u. $packet\_ID$ is used by u to monitor packet transmission from v to next node. A MAC is appended at the end of the packet to detect any modification. The input to the MAC is everything before the MAC.
2) Node v sends the packet to its parent node in the tree. To guarantee the delivery, each L-sensor is responsible for confirming that its successor has successfully forwarded the packet. This may be implemented by the transmitter monitoring the packet just sent out to the next node and overhearing if that node has passed it on within a time period using the $packet\_ID$ field. The acknowledgement scheme reduces the impact of channel or node error and can detect selective forwarding attack.
3) If u does not get an acknowledgement within a certain time period, u will re-transmit the packet to v. If the transmission to v fails again, u will send the packet to a backup parent node.
4) The process continues until the data packet reaches the cluster head H.

B. Secure Inter-Cluster Routing

Routing among clusters (from an H-sensor to the BS) is referred to as inter-cluster routing. In the following, we present the secure inter-cluster routing scheme. Cluster heads know the location of the BS (e.g., from a BS broadcast). After cluster formation, each cluster head exchanges location information with neighbor cluster heads. During route discovery, a cluster head draws a straight line L between itself and the BS, based on the locations of the BS and itself. In Fig. 1, the double dotted line is line L. Line L intersects with a serial of clusters, and these clusters are denoted as $C_0, C_1, ..., C_k$, which are referred to as *Relay Cells*. The packet is forwarded from the source cluster head to the BS via cluster heads in the *Relay Cells*. A secure data forwarding scheme similar to the one above (subsection III-A) is used to provide security to communications between two H-sensors (or an H-sensor and the BS).

H-sensors are more reliable nodes than L-sensors. However, an H-sensor may also fail because of various reasons, such as harsh environment, or destroyed by an adversary. We use Fig. 1 to describe a self-healing scheme for H-sensor failures. If any cluster head in the *Relay Cells* is unavailable, then a backup path is used. A backup path is set up as follows: The current cluster head (say R_1) draws a straight line L between itself and the BS, and line L intersects with several cells $C_1^{'}, ..., C_{k-1}^{'}, C_k$. If the next cell is the cell having the failed cluster head, R_1 will use a detoured path to avoid the cell. Otherwise, the sequence of new cells $C_1^{'}, ..., C_{k-1}^{'}, C_k$ will be the new *Relay Cells*.

IV. Probability of H-Sensors in a Certain Area

To ensure the TTSR protocol works well, it is important to have most areas of an HSN being covered by (i.e., within the transmission range of) one or more H-sensors. If the locations of H-sensors are controllable (e.g., distributed by human), then it is easy to have each point of the network being covered by one or more H-sensors. Below we consider more general case where H-sensors are randomly deployed in the network (e.g., distributed by an airplane). The network is divided into several equal-sized cells with side length $a = R/2$, where R is the transmission range of an H-sensor. Assume that there are m cells and totally n H-sensors deployed in the network. Let F be the set of all cells. The Vapnik-Chervonenkis (VC) dimension of F is 3. We use the following VC-dimension Theorem [28] to obtain the probability of having an H-sensor in a cell.

The VC Theorem: If F is a set of finite VC-dimension VC_d(F), and $\{X_i\}$ is a sequence of i.i.d. (independently and identically distributed) random variables with common probability distribution P, and denote E as a element of F, $E \in F$, then for every $\varepsilon, \delta > 0$, we have:

$$P(\sup_{E \in F} |\frac{1}{n} \sum_{i=1}^{n} I(X_i \in E) - P(E)| \leq \varepsilon) > 1 - \delta \quad (1)$$

when

$$n > \max\{\frac{8 \times VC\_d(F)}{\varepsilon} \log \frac{16e}{\varepsilon}, \frac{4}{\varepsilon} \log \frac{2}{\delta}\}.$$

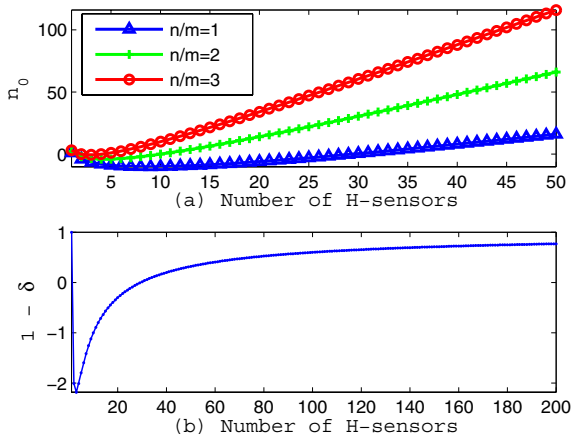

Fig. 2. The curve of n_0 and $1-\delta$.

Assume that H-sensors are uniformly and randomly distributed in the network, and then we can apply uniform convergence in the weak law of large numbers. We have, $P(E)$ = the average density of H-sensors per cell = n/m. We choose $\varepsilon(n) = \delta(n) = 20 \times \log n/n$.

Denote $n_1 = \frac{8 \times VC\_d(F)}{\varepsilon} \log \frac{16e}{\varepsilon} = \frac{24}{\varepsilon} \log \frac{16e}{\varepsilon}$, and $n_2 = \frac{4}{\varepsilon} \log \frac{2}{\delta}$. When $n > 10$, we have $n > n_1$ and $n > n_2$, which means that $n > \max\{\frac{8 \times VC\_d(F)}{\varepsilon} \log \frac{16e}{\varepsilon}, \frac{4}{\varepsilon} \log \frac{2}{\delta}\}$ is satisfied when $n > 10$. Therefore, when $n > 10$, we have, $P(\sup_{E \in F} |\frac{1}{n} \sum_{i=1}^{n} I(X_i \in E) - P(E)| \leq \varepsilon) > 1 - \delta$, i.e.,

$$P(\sup_{E \in F} |\frac{\text{Number of H-sensors in E}}{n} - \frac{n}{m}| \leq \varepsilon) > 1 - \delta \Rightarrow$$

$$P(\text{Number of H-sensors in E} \geq n(\frac{n}{m} - \varepsilon)) > 1 - \delta \quad (2)$$

The probability $P(E) = n/m$ depends on the ratio between n and m. In Fig. 2(a), we plot the curve $n_0 = n(n/m - \varepsilon) = n(2 - 20 \log n/n)$ for different values of n/m. Fig. 2(a) shows that the larger n/m, the larger the value of n_0 is for a fixed n (number of H-sensors). Note $n_0 > 0$ means that the probability in equation (2) is the probability of having at least one H-sensor. For example, when $n/m = 2$, $n_0 > 0$ when $n > 11$. The curve of $1 - \delta(n)$ is plotted in Fig. 2(b), and it shows that $1 - \delta(n)$ is always greater than zero when $n > 30$. The value of $1 - \delta(n)$ increases as n increases and goes to 1. This can be easily verified, i.e., $1 - \delta(n) = 1 - 20 \log n/n \to 1$ as $n \to \infty$. Hence, we have the following Theorem.

Theorem 1: When sufficient number of H-sensors are randomly deployed in a field, (e.g., $n > 11$ and $n/m \geq 2$, where n and m are the numbers of H-sensors and cells, respectively), the probability of having at least one H-sensor in each cell is larger than $1 - 20 \log n/n$, and this probability goes to 1 as $n \to \infty$. That is, when n is sufficiently large, there is a very high probability that each cell has at least one H-sensor.

Proof: The proof follows from the above discussion.

To sum up, in this section, we show that when the number of H-sensors is large, the probability of having at least one H-sensor in a cell is high. This high probability ensures the good performance of TTSR.

V. Security Analysis

In this section, we analyze the security of TTSR. Due to the limited storage in L-sensors, all cryptographic primitives, i.e., encryption, message authentication code, random number generator, use a single block cipher for code reuse. In the following experiments, RC5 [21] is used as the block cipher. The security configuration is discussed below.

- **Data Authentication** and **Data Integrity** are achieved by MAC, i.e., a send and a receiver computes a MAC with their shared-key.
- **Data Confidentiality** is provided by symmetric encryption.

TTSR routing protocol can defend against typical attacks on sensor network routing. Attacks on sensor networks have been discussed in several papers, e.g., [14], [15], [22], [23]. Most network layer attacks against sensor networks fall into one of the following categories: manipulating routing information [14], selective forwarding [14], Sybil [22], Sink-hole [15], wormhole [23], and Hello flooding (unidirectional) attacks [15]. Brief descriptions of these attacks can be found in [24]. In the following, we discuss how TTSR can defend against various attacks on sensor network routing.

- **Defending against the Sybil Attack**: In Sybil attack [22], a single node presents multiple identities to other nodes in the network. Authentication is used to ensure one node cannot pretend to be other nodes, i.e., when a sensor node u sends a packet to another node v, u must present a MAC computed using the shared pairwise key $K_{u,v}$ between u and v. Since the pairwise key $K_{u,v}$ is only known by u and v, no adversary node can pretend to be node u (unless u is captured and the keys in u are obtained by the adversary). Thus, the Sybil attack does not work.
- **Defending against the Wormhole and Sink-hole Attacks**: TTSR routing includes two parts - intra-cluster routing and inter-cluster routing. For intra-cluster routing, an L-sensor only sends the data to its parent node of the (MST or SPT) tree, and the parent-child relationship is determined by the cluster head. For inter-cluster routing, given the locations of the H-sensor and the BS, a serial of cells is determined as *Relay Cells*, and the packet is forwarded only by H-sensors in the *Relay Cells*. Other nodes should not participate in routing. An adversary is not able to route in TTSR, and therefore TTSR is resistant to wormhole attack and sink-hole attack.
- **Defending against the Manipulating Routing Information Attack**: In TTSR, the routing information is distributed by the cluster head. Since a cluster head is an H-sensor with tamper-resistant hardware, it is well protected and can not be compromised by the adversary. A cluster head appends keyed MAC to each routing control message. Only the L-sensor and the cluster head know the key used to generate the MAC, and thus an adversary is not able to send false routing information.
- **Defending against the Selective Forwarding Attack**: H-sensors are protected by the tamper-resistant hardware, hence H-sensors can not be compromised, and the selective forwarding attack can not be launched on H-sensors.

However, a selective forwarding attack may happen on an L-sensor. For example, a powerful adversary always serves as a relay node in a cluster, and she can selectively forward some packets while dropping other packets. The $packet\_ID$ field is used to defend this attack. Recall that each relay L-sensor is responsible for confirming that its successor has successfully forwarded the packet by overhearing the transmission. The $packet\_ID$ field is used to identify the particular packet. If a node selectively drops a packet, this will be detected by the up-stream sender.

- **Defending against the Hello Flood Attack** is achieved by the two-way handshake protocol in subsection III-A.

VI. Evaluation of Routing Performance

In this section, we present the performance evaluation of routing efficiency and effectiveness of TTSR. QualNet [25] is used to compare the routing performance of TTSR with a popular sensor network routing protocol - Directed Diffusion (DD) [1], when there is no attack placed on the sensor network. In the simulation, the underlying medium access control protocol is IEEE 802.11 Distributed Coordination Function (DCF). The default simulation testbed has 1 base station and 300 L-sensors randomly distributed in a $300m \times 300m$ area. For TTSR, there are additional 20 H-sensors. The transmission range of an L-sensor and an H-sensor is 60m and 150m, respectively. Each simulation run lasts for 600 seconds, and each result is averaged over five random network topologies. Each L-sensor generates one data packet every 5 seconds. Each data packet is 64 bytes. The network is divided into equal-sized cells, and the side length of a cell is set as $a = r/2 = 60m/2 = 30m$. Du [26] studied the effect of different cell size on routing performance. One of the results is that $r/2$ is a good value for the cell size that tradeoffs the routing performance and the number of cells.

For simulations presented in this section, no data fusion is performed, and a distributed Shortest Path Tree (SPT) algorithm is used for intra-cluster routing in TTSR. In the experiments, the energy consumption and routing overhead of TTSR include those from all cryptographic primitives (i.e., encryption/decryption, MAC computation, random number generator) in TTSR. Note that DD does not use any cryptographic primitives and does not provide security to routing. We consider energy consumptions for two kinds operations in sensor networks, i.e., communications and running cryptographic primitives. To facilitate comparisons with DD, we use the same energy model for L-sensors as adopted in DD's implementation in ns-2.1b8a [1]. The transmitting, receiving and idling power consumption rates of an L-sensor are 0.66W, 0.395W and 0.035W, respectively. The transmitting, receiving and idling power consumption rates of an H-sensor are set as 2.64W, 1.58W and 0.14W, respectively. We set the power consumption rates of RC5 according to [27], and (for both H-sensors and L-sensors) the rates of encryption, MAC calculation, and random number generator are 0.65W, 0.48W and 0.36W, respectively.

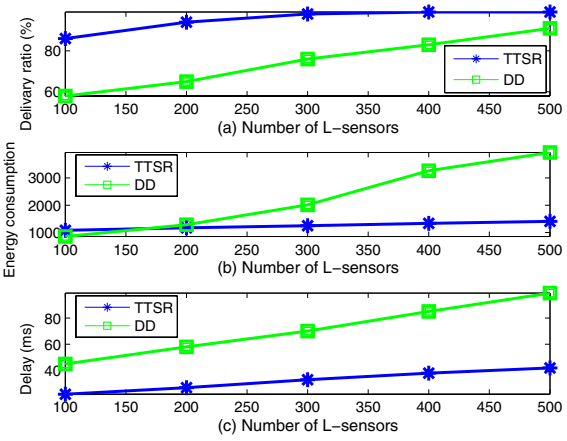

Fig. 3. Routing performance under different node densities.

A. Routing Performance under Different Node Densities

First, we compare the delivery ratio, energy consumption and end-to-end delay for different node densities. For the fixed $300m \times 300m$ routing area, the number of L-sensors varies from 100 to 500 with an increment of 100. The number of H-sensors does not change. The delivery ratios under TTSR and DD are plotted in Fig. 3(a). We observe that the delivery ratio of both TTSR and DD increases as the L-sensor density increases. In TTSR, when L-sensor density increases, there are more L-sensors in each cluster and more candidates to relay packets to the cluster head. This is why the delivery ratio under TTSR increases as L-sensor density increases. In DD, there are more sensors to forward packets when node density increases, and thus the delivery ratio of DD also increases. Fig. 3(a) shows that TTSR has higher delivery ratio than DD. In TTSR, an L-sensor only needs to send packets to its nearby cluster head, and the rest transmissions are done by the H-sensor backbone. From the same L-sensor to the BS, TTSR routing requires fewer hops than DD. Also H-sensors have higher data rate and are more reliable than L-sensors. Thus, the delivery ratio of TTSR is higher than that of DD.

The total energy consumptions of TTSR and DD are reported in Fig. 3(b). The energy consumptions of both protocols grow with node density. In TTSR, the main reason is that more power is dissipated for overhearing when every L-sensor has more neighbors, and thus the energy consumed by TTSR only increases a little bit when node density is high. However, the energy consumption of DD increases much faster than TTSR, and it becomes very large when node density is high. This is because in DD more and more nodes are involved in disseminating "*interest*" and "*gradient*" when node density increases [1]. The end-to-end delay is compared in Fig. 3(c). As we can see, TTSR also has smaller end-to-end delay than DD for all the tested sensor density. The reason is that the same pair of source-destination in TTSR uses fewer hops of transmissions than that in DD.

B. Routing Performance for Different Source-BS Distances

Fig. 4 reports the delivery ratio and energy consumption for different source - BS distances. The delivery ratio of TTSR

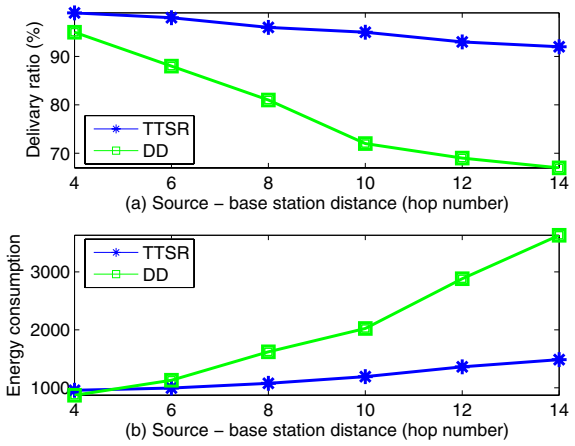

Fig. 4. Routing performance for different source-BS distances.

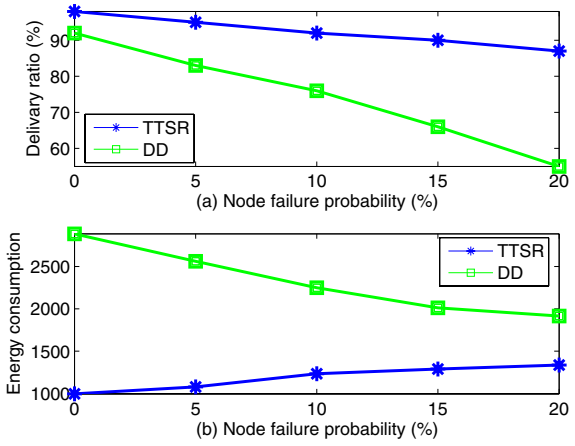

Fig. 5. Routing performance under different node failure probabilities.

and DD slightly decreases for larger source - BS distance, but DD drops much faster than TTSR. For any source - BS distance, the delivery ratio of TTSR is higher than DD, and the reason is similar to that in subsection VI-A. TTSR utilizes H-sensors for most transmissions and thus has less hop count than DD. The total energy consumed by TTSR and DD increases as distance increases, as shown in Fig. 4(b). However, the increase in DD is much faster than TTSR. In DD, more nodes participate in routing as the source-base station distance increases, and hence much more energy is consumed. In TTSR, only the number of L-sensors involved in the intra-cluster routing increases, while the number of H-sensors for the inter-cluster routing remains the same, so the energy consumption only increases slightly in TTSR.

C. Routing Performance for Different Node Failure Probabilities

Fig. 5 shows the change of delivery ratio and energy consumption for different L-sensor failure probability p. Since H-sensors are more reliable than L-sensors, the failure probability of H-sensors is set as $1/3$ of p. The delivery ratios of both TTSR and DD decrease as sensor failure probability increases. However, the decrease in TTSR is much slower than DD. For the same source-BS pair, fewer sensors are in the route in TTSR that those in DD. In addition, H-sensors are less likely to fail. Fig. 5(a) shows that the delivery ratio of TTSR is always higher than 90% when p is less than 15%. As Fig. 5(b) shows that the energy consumption of DD decreases as p increases, since fewer sensors are involved in routing as more nodes fail. The energy consumption of TTSR increases a little bit as p increases; this is mainly due to node failures that cause re-transmissions and additional security operations in TTSR.

In summary, our simulation experiments show that TTSR has a higher delivery ratio, a smaller end-to-end delay and lower energy consumption than Directed Diffusion, even though Directed Diffusion does not run any security primitives. TTSR achieves better routing performance by utilizing powerful H-sensors. It is noted that H-sensors are more expensive than L-sensors. For example, the current price of a MICA2 and a Stargate processor/radio board is $\$125$ and $\$425$, respectively [7]. Thus, using an HSN design does increase the cost of a sensor network. However, since the number of H-sensors in an HSN is small, the increased cost is not large.

VII. Conclusions

In this paper, we presented a novel secure routing protocol for heterogeneous sensor networks (HSNs), namely Two-Tier Secure Routing (TTSR) protocol. Clusters are formed in an HSN and H-sensors serve as cluster heads. TTSR consists of a secure intra-cluster routing scheme and a secure inter-cluster routing scheme. For intra-cluster routing, a minimum spanning tree or the shortest path tree is formed among L-sensors in a cluster for data forwarding. For inter-cluster routing, packets are forwarded by H-sensors in the *Relay Cells* along the direction from source to the base station. Our security analysis shows that TTSR can defend against several sophisticated routing attacks. The nature of TTSR (tree-based routing and relay via *Relay Cells*) makes it resistant to spoofed routing information, selective forwarding, sink-hole and wormhole attacks. The two-way handshake can defend against Hello flood attack. Our simulations demonstrated the good routing performance of TTSR, i.e., TTSR has a higher delivery ratio, a lower end-to-end delay and smaller energy consumption than a popular non-secure routing protocol - Directed Diffusion.

References

[1] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks," in *Proc. ACM MOBICOM*, Aug. 2000, pp. 56–67.
[2] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocols for wireless microsensor networks," in *Proc. Hawaiians Int'l Conf. Syst. Science*, Jan. 2000, pp. 3005–3014.
[3] C. Karlof, N. Sastry, and D. Wagner, "TinySec: A link layer security architecture for wireless sensor networks," in *Proc. 2nd ACM Conf. Embedded Networked Sensor Syst.*, Nov. 2004, pp. 162–175.
[4] P. Gupta and P. R. Kumar, "The capacity of wireless networks," *IEEE Trans. Inform. Theory*, vol. 46, no. 2, pp. 388–404, Mar. 2000.
[5] K. Xu, X. Hong, and M. Gerla, "An ad hoc network with mobile backbones," in *Proc. IEEE ICC*, Apr. 2002, 3138–3143.
[6] L. Girod, T. Stathopoulos, N. Ramanathan, et al., "A system for simulation, emulation, and deployment of heterogeneous sensor networks," in *Proc. 2nd ACM Conf. Embedded Networked Sensor Systems*, Nov. 2004, pp. 201–213.
[7] Crossbow Technology Inc. [Online]. Available: www.xbow.com
[8] V. Mhatre, C. P. Rosenberg, D. Kofman, et al. "A minimum cost heterogeneous sensor network with a lifetime constraint," *IEEE Trans. Mobile Computing*, vol. 4, no. 1, pp. 4–15, Jan. 2005.

[9] E. Duarte-Melo and M. Liu, "Analysis of energy consumption and lifetime of heterogeneous wireless sensor networks," in *Proc. IEEE Globecom*, Nov. 2002, pp. 21–25.
[10] X. Du and Y. Xiao, "Energy efficient chessboard clustering and routing in heterogeneous sensor network," *Int. J. Wireless Mobile Computing (IJWMC)*, vol. 1, no. 2, pp. 121-130, Jan. 2006.
[11] X. Du and F. Lin, "Maintaining differentiated coverage in heterogeneous sensor networks," *EURASIP J. Wireless Commun. Networking*, no. 4, pp. 565–572, Oct. 2005.
[12] M. Yarvis, N. Kushalnagar, H. Singh, et al., "Exploiting heterogeneity in sensor networks," in *Proc. IEEE INFOCOM*, Mar. 2005, pp. 878–890.
[13] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in *Proc. 10th ACM Conf. Computer Commun. Security*, Nov. 2003, pp. 52–61.
[14] A. D. Wood, and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, Oct. 2002.
[15] C. Karlof and D. Wagner, "Secure routing in sensor networks: Attacks and countermeasures," in *Proc. IEEE 1st Int. Workshop Sensor Network Protocols Applications*, May 2003, pp. 113–127.
[16] X. Du, Y. Xiao, M. Guizani, and H. H. Chen, "An effective key management scheme for heterogeneous sensor networks," *Ad Hoc Networks (Elsevier)*, vol. 5, no. 1, pp. 24–34, Jan. 2007.
[17] L. Lazos and R. Poovendran, "SeRLoc: Secure range-independent localization for wireless sensor networks," in *Proc. ACM Workshop Wireless Security*, Oct. 2004, pp. 21–30.
[18] R. Cristescu and B. Beferull-Lozano, "Lossy network correlated data gathering with high-resolution coding," *IEEE/ACM Trans. Networking*, vol. 14, pp. 2817–2824, June 2006.
[19] B. Karp and H. T. Kung, "Gpsr: Greedy perimeter stateless routing for wireless networks," in *Proc. 6th ACM MOBICOM*, Aug. 2000, pp. 243–254.
[20] "Kruskal's Algorithm" [Online]. Available: http://www.cs.rutgers.edu/ chvatal/notes/mst.html
[21] R. L. Rivest, "The RC5 encryption algorithm," in *Proc. Leuven Workshop Fast Software Encryption*, Jan. 1995, pp. 86–96.
[22] J. R. Douceur, "The Sybil attack," in *Proc. IPTPS*, Mar. 2002, pp. 251–260.
[23] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole detection in wireless ad hoc networks," Technical Report TR01-384, Department of Computer Science, Rice University, June 2002.
[24] X. Du, Y. Xiao, H. H. Chen, and Q. Wu, "Secure cell relay routing protocol for sensor networks," *Wireless Commun. Mobile Computing (Wiley)*, vol. 6, no. 3, pp. 375–391, May 2006.
[25] "QualNet Network Simulator, The Scalable Network Technology" [Online]. Available: www.qualnet.com
[26] X. Du, "QoS routing based on multi-class nodes for mobile ad hoc networks," *Ad Hoc Networks (Elsevier)*, vol. 2/3, pp. 241–254, July 2004.
[27] Q. Xue and A. Ganz, "Runtime security composition for sensor networks," in *Proc. IEEE Veh. Technol. Conf.*, Oct. 2003, pp. 105–111.
[28] M. C. Laskowski, "Vapnik-Chervonenkis classes of definable sets," *J. London Mathematical Society*, vol. 45, no. 2, pp 377–384, 1992.

Xiaojiang (James) Du (M'03) is an assistant professor in the Department of Computer Science, North Dakota State University. Dr. Du received his B.E. degree from Tsinghua University, Beijing, China in 1996, and his M.S. and Ph.D. degrees from University of Maryland, College Park in 2002 and 2003, respectively, all in electrical engineering. His research interests are heterogeneous wireless sensor networks, security, wireless networks, computer networks, and network and systems management. Dr. Du is an Associate Editor of *Wiley Wireless Communication and Mobile Computing*, and the *InterScience International Journal of Sensor Networks*.

Mohsen Guizani (SM'99) is currently a full professor and chair of the Computer Science Department at Western Michigan University. He has authored or co-authored over 180 technical papers in major international journals and conferences. His research interests include computer networks, design and analysis of computer systems, wireless communications, and optical networking. He currently serves on the editorial boards of many national and international journals. He is the founder and Editor-In-Chief of *Wiley Wireless Communications* and the *Mobile Computing Journal*.

Yang Xiao (SM'04) is currently with the Dept. of Computer Science at The Univ. of Alabama. Dr. Xiao was a voting member of the IEEE 802.11 Working Group from 2001 to 2004. He currently serves as Editor-in-Chief for the *International Journal of Security and Networks* (IJSN), the *International Journal of Sensor Networks* (IJSNet), and the *International Journal of Telemedicine and Applications* (IJTA). His research areas are wireless networks, mobile computing, network security, and telemedicine. He has published more than 200 papers in major journals (more than 50 in various IEEE Journals/magazines), refereed conference proceedings, and contributed book chapters related to these research areas.

Hsiao-Hwa Chen (SM'00) was the founding director of the Institute of Communications Engineering, National Sun Yat-Sen University, Taiwan. He has authored or co-authored over 200 technical papers in major international journals and conferences, and six books in the areas of communications. He has served as symposium co-chair of major international conferences, including IEEE VTC, ICC, Globecom, WCNC, etc. He served or is serving as an Editor and/or Guest Editor of many international journals. He is an Adjunct Professor of Zhejiang University, and Shanghai Jiao Tung University, China.