Report on Wireless Communications and Networks Project 14
Routing in Sensor Networks

By Group One
Chen Guo, Chen Jing, Wang Qingsi, Xu Miao

Part One

ASYMPTOTIC CONNECTIVITY IN HIERARCHICAL CLUSTERING ARCHITECTURE OF WIRELESS SENSOR NETWORK

WANG QINGSI, CHEN GUO

1. Introduction

As in many other sorts of wireless networks, the energy-saving issue in wireless sensor networks (WSN) is of significance. It's dominant in protocol designing for sensor networks, given the limited power capacity of sensor nodes.

Some researches have already pointed out that the main energy consumption in wireless sensor networks comes from the transmission process, while the computation consumes a much smaller amount of energy. Besides, nodes in wireless communication networks including WSN, share a common communication medium. Thus, signal interference among nodes exists and results in reduced signal to noise ratio at the latter receivers and in lowering of networks' information-processing capacity. Hence, it becomes essential to control the transmitter power such that the information signals reach their intended receivers, while saving crucial energy and causing minimal interference for other receivers sharing the same channel.

Gupta and Kumar have done important work on the transmitting power control problem and achieved some interesting results in critical power for asymptotic connectivity (Gupta and Kumar (1998) [1] and the references therein). That is, for a wireless network formed by a group of mobile nodes which communicate with each other over a wireless channel and without any centralized control, there exists a lower bound of power at which each node needs to transmit, so as to guarantee for each node a path to every other node in the network.

Here we present the critical power problem more precisely in the fashion how Gupta and Kumar present it: Let $\mathcal{D}$ be a disc in $\mathfrak{R}^2$ having unit area. Let $\mathcal{G}(n, r(n))$ be the network (graph) formed when n nodes are placed uniformly and independently in $\mathcal{D}$, and two nodes i and $j$can communicate with each other if the distance between them is less than $r(n)$. Then Gupta and Kumar have proved that *graph* $\mathcal{G}(n, r(n))$*, with* $\pi r(n)^2 = \frac{\log n + c(n)}{n}$ *is connected with probability one as* $n \to +\infty$ *if and only if* $c(n) \to +\infty$.

In the problem presented by Gupta and Kumar above, we refer to the networks assumed in this problem as *flat* networks, since this type of networks is not hierarchically organized, which means nodes within this type of networks are homogenous in function and they can share their information mutually. A connected flat network is shown in Figure 1.

However, in wireless sensor networks which normally have sinks or base stations to collect data from monitoring nodes, although there are also many kinds of network architectures, clustering architecture is proved to be energy efficient by surveys [2]. Clustering architectures normally organize homogenous nodes into

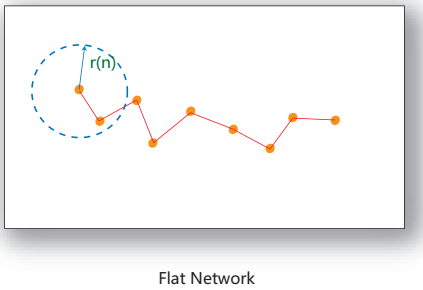

FIGURE 1. A hierarchical network

clusters, and a cluster head is selected for each cluster. Typically, cluster heads are selected randomly within the whole network dynamically for the sake of energy-consuming balance, like LEACH [3] and other prototols alike do in WSN. Non-cluster-head nodes, i.e., cluster-members, are responsible for the monitoring task, and they *only* communicate with one of the cluster-heads within its communication range. Cluster-heads are responsible to distribute the information collected by the members to sinks. This basic clustering architecture is demonstrated in Figure 2.

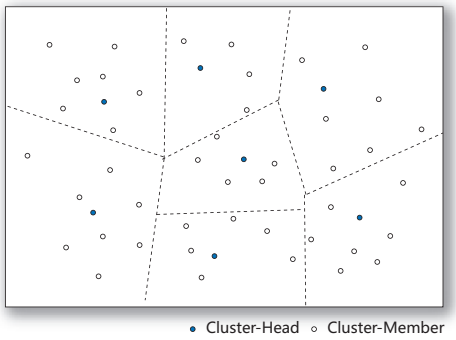

FIGURE 2. A scenario of basic clustering

Furthermore, let us defined clusters shown in Figure as the 1st order clusters. Then, cluster-head nodes can be organized into higher order clusters, and a 2nd order cluster-head can be selected within each 2nd cluster. If we regard the 1st order cluster-members as being in one layer, we have a higher layer formed by the 2nd order cluster-members, i.e., the 1st order cluster-heads. This clustering process can carry on for several rounds to form *hierarchical* networks. In this hierarchical clustering architecture, member nodes in the 1st order clusters take the task of information collection, and cluster-heads in any order are responsible for data relaying and cluster organization.

The information transmission from the bottom layer nodes requires a multi-hop path across successive layers, and each node's cluster-head must be the next hop in the path. Then we define this path as a multi-layer path. The data is directly relayed by a cluster-head in each layer. The hierarchy-forming and data relaying process is shown in Figure 3.

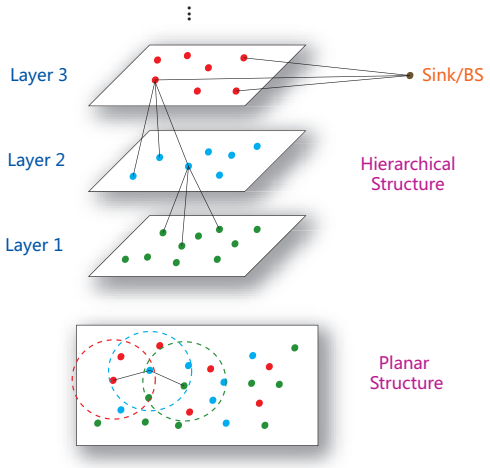

FIGURE 3. A hierarchical network

As in *flat* networks, nodes in hierarchy networks can only communicate to other nodes within a communication range $r(n)$. Nevertheless, instead of the connectivity among nodes in a single layer presented before, it's the connectivity between nodes in every two neighboring that concerns us. Since a kth layer is formed stochastically, a multi-layer path from a bottom node to a top head may not exist, once a relaying node cannot find a cluster head in the next layer within its communication range $r(n)$. Let $\mathcal{G}_c(n, r(n))$ be the network (graph) formed by the graph $\mathcal{G}(n, r(n))$ with nodes organized in a clustering fashion. Then the problem is to determine $r(n)$ which guarantees that $\mathcal{G}_C(n, r(n))$ is asymptotically connected in the way we discussed above with probability one.

In the following part of this chapter, we show that graph $\mathcal{G}_c(n, r(n))$, with $\pi r(n)^2 = \frac{\log n + c(n)}{n}$ is connected in clustering fashion with probability one as $n \to +\infty$. Our work is mainly based on the result achieved by Gupta and Kumar (1998).

2. Necessary Condition on $r(n)$ for Connectivity

In this section we derive necessary conditions on the radio range of a node in the hierarchical network for asymptotic connectivity. We will also neglect edge effects resulting due to a node being close to the boundary of $\mathcal{D}$, just as Gupta and Kumar did in their primary proof, and we will adopt the main results they achieved under this condition.

Let $P_{dc}(n, r(n))$ denote the probability that $\mathcal{G}_C(n, r(n))$ is disconnected.

Theorem 2.1. *If* $\pi r(n)^2 = \frac{\log n + c(n)}{n}$, *then*

$$\liminf_{n\to\infty} P_{dc}(n, r(n)) \geq p_1 \cdot e^{-c}(1 - e^{-2c}), \tag{2.1}$$

where $c = \lim_{n\to\infty} c(n)$, p_1 *is the probability of a node to be in layer 1 and* $p_1 \neq 0$.

Proof. Similar to the proof of *Theorem 2.1* in Gupta and Kumar (1998), we first study the case where $\pi r(n)^2 = \frac{\log n + c}{n}$ for a fixed c.

$$\begin{aligned} P_{dc}(n, r(n)) &\geq P(\{\mathcal{G}_c(n, r(n) \text{ has a isolated node in layer 1}\}) \\ &= \sum_{i=1}^{n} P(\{\text{i is the only isolated node in } \mathcal{G}(n, r(n))\}) \\ &\quad \cdot P(\{\text{i is a node in layer 1}\}) \\ &= p_1 \cdot \sum_{i=1}^{n} P(\{\text{i is the only isolated node in } \mathcal{G}(n, r(n))\}) \\ &\geq p_1 \cdot \Bigg[\sum_{i=1}^{n} P(\{\text{i is an only isolated node in } \mathcal{G}(n, r(n))\}) \\ &\quad - \sum_{j \neq i} P(\{\text{i and j are isolated nodes in } \mathcal{G}(n, r(n))\})\Bigg]. \end{aligned}$$

Referring to the proof of *Theorem 2.1* in Gupta and Kumar (1998), we can obtain that for any fixed $\theta < 1$ and $\epsilon > 0$,

$$\begin{aligned} P &= \sum_{i=1}^{n} P(\{\text{i is an only isolated node in } \mathcal{G}(n, r(n))\}) \\ &\quad - \sum_{j \neq i} P(\{\text{i and j are isolated nodes in } \mathcal{G}(n, r(n))\}) \\ &\geq \theta e^{-c} - (1 + \epsilon) e^{-2c}, \end{aligned}$$

for all $n > N(\epsilon, \theta, c)$. Thus,

$$P_{dc}(n, r(n)) \geq p_1 \cdot [\theta e^{-c} - (1 + \epsilon) e^{-2c}],$$

for all $n > N(\epsilon, \theta, c)$. Now, following the same steps in the proof of *Theorem 2.1* in Gupta and Kumar (1998), consider the case where is c is a function $c(n)$ with $\lim_{n\to\infty} c(n) = \bar{c}$, we have

$$\liminf_{n\to\infty} P_{dc}(n, r(n)) \geq p_1 \cdot [\theta e^{-(\bar{c}+\epsilon)} - (1 + \epsilon) e^{-2(\bar{c}+\epsilon)}],$$

for all $\epsilon > 0$ and $\theta < 1$. Therefore,

$$\begin{aligned} \liminf_{n\to\infty} P_{dc}(n, r(n)) &\geq p_1 \cdot \sup[\theta e^{-(\bar{c}+\epsilon)} - (1 + \epsilon) e^{-2(\bar{c}+\epsilon)}] \\ &= p_1 \cdot e^{-c}(1 - e^{-2c}). \end{aligned}$$

□

Necessary condition: Graph $\mathcal{G}_c(n, r(n))$ is asymptotically disconnected with positive probability if $\pi r(n)^2 = \frac{\log n + c(n)}{n}$ and $\limsup_{n\to\infty} c(n) < +\infty$.

3. Sufficient Condition on $r(n)$ for Connectivity

Like the denotation in Gupta and Kumar (1998), let $P^{(k)}(n, r(n)), k = 1, 2, ...$ denote the probability that a graph $\mathcal{G}(n, r(n))$ has at least one order-k component, which means a set of k nodes which form a connected set, but which are not connected with any other node. This concept is demonstrated in Figure 4.

Then we redefine the order-k component in graph $\mathcal{G}_c(n, r(n))$ as a set of k nodes which consist a order-k component in graph $\mathcal{G}(n, r(n))$ and happens to form a

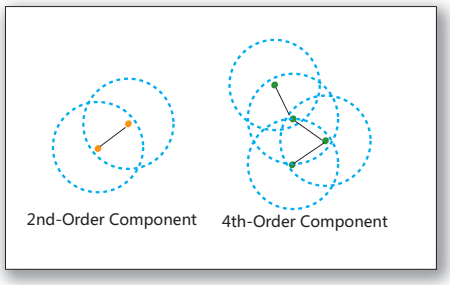

FIGURE 4. A 6-node flat network disconnected with a 2nd-order component and a 4th-order component

multi-layer path across k layers as well. Let $P_c^{(k)}(n, r(n)), k = 1, 2, ...m-1$, denote the probability that a graph $\mathcal{G}_c(n, r(n))$ with m layers has at least one order-k component. Figure 5 shows an example of order-k components in graph $\mathcal{G}_c(n, r(n))$. From this figure we can find that the node in layer 2 on the left is not within the range of the node in layer 3, and thus it forms a 2nd-order component with the node to its left in layer 1, while the entire network is connected if it's treated as a *flat* network.

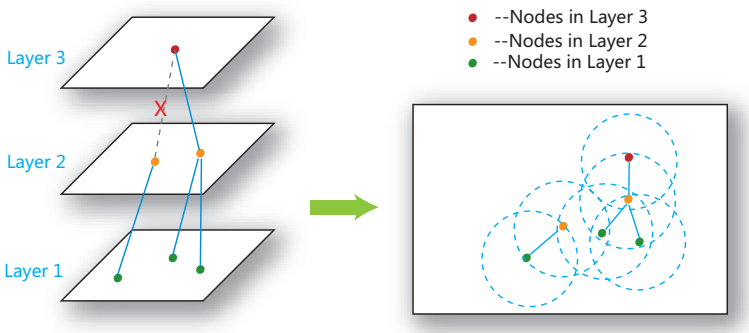

FIGURE 5. A hierarchical network disconnected with a 2nd-order component

Theorem 3.1. *If* $\pi r(n)^2 = \frac{\log n + c(n)}{n}$, *then*

$$\limsup_{n\to\infty} P_c^{(k)}(n, r(n)) \leq 4e^{-c}, \tag{3.1}$$

where $c = \lim_{n\to\infty} c(n)$.

Proof. From the definition of $P_c^{(k)}(n, r(n)), k = 1, 2, ...m-1$, we have

$$\begin{aligned} P_c^{(k)}(n, r(n)) &\leq P^{(k)}(n, r(n)) \cdot P(\{i_1,\ i_2 ... i_k \text{ consist a k-hop path across k layers}\}) \\ &\leq P^{(k)}(n, r(n)). \end{aligned}$$

Since $P^{(k)}(n, r(n)) \leq P_d(n, r(n))$, for $k = 1, 2, ..., n-1$, with the *Theorem 3.1* in Gupta and Kumar (1998) we can obtain

$$\begin{aligned} \limsup_{n\to\infty} P_c^{(k)}(n, r(n)) &\leq \limsup_{n\to\infty} P^{(k)}(n, r(n)) \\ &\leq \limsup_{n\to\infty} P_d(n, r(n)) \\ &\leq 4e^{-c}. \end{aligned}$$

□

Sufficient condition: Graph $\mathcal{G}_c(n, r(n))$ is asymptotically connected with probability one for $\pi r(n)^2 = \frac{\log n + c(n)}{n}$ if c(n) $\to +\infty$.

Corollary 3.2. *Graph $\mathcal{G}_c(n, r(n))$, with $\pi r(n)^2 = \frac{\log n + c(n)}{n}$ is connected in clustering fashion with probability one as $n \to +\infty$ if and only if $c(n) \to +\infty$.*

4. Conclusion

In this report, we have derived the critical range of nodes randomly placed in a disc of unit area and organized in a hierarchical clustering fashion. Our work is mainly based on the critical range of nodes in the $flat$ network found by Gupta and Kumar. We have proved that the critical range $r(n)$ for the hierarchical clustering architecture is the same as that shown by Gupta and Kumar. Our future work includes proving this problem considering the edge effect which we neglect in the current work.

References

1. Piyush Gupta and P.R Kumar, "*Critical power for asymptotic connectivity in wireless network*," in Stochastic Analysis, Control, Optimization and Applications: A Volume in Honor of W.H. Fleming, W.M. McEneany, G. Yin, and Q. Zhan, Eds. 1998, pp. 547 - 566, Birkhauser, Boston.
2. Qiangfeng Jiang and D. Manivannan, "*Routing Protocols for Sensor Networks*," in Consumer Communications and Networking Conference, 2004, CCNC 2004, pp. 93 - 98.
3. W. Heinzelman, A. Chandrakasan and H. Balakrishnan, "*Energy- efficient Communication Protocol for Wireless Micro Sensor Networks*", in Proc. of the 33rd Annual Hawaii International Conf. on System Sciences, 2000, pp. 3005C3014.

Part Two

IMPROVEMENT OF DATA FUSION IN LEACH

CHEN JING

1. Motivation

Wireless sensor networks comprises of hundreds or even thousands of small nodes. These nodes, with limited computing, communicating and sensing capabilities as well as limited energy, can make the best use of themselves to gather data from sensor nodes to Base Station by using excellent data fusion algorithms in order to gain the lifetime as long as possible. Data fusion is an important part of sensor network protocol, as sensory data gathered have redundant information which cost unneeded energy.

The Photogrammetry and Remote Sensing Community, in which Wald proposes a definition of Data Fusion [1]: Data fusion is formal framework in which are expressed the means and tools for the alliance of data originating from different sources. It aims at obtaining information of greater quality; the exact definition of greater quality will depend upon the application.

The data fusion in LEACH will generally be expressed in Section 2. FCM Algorithm is a good algorithm for cluster-based sensor data fusion, we will talk about that in Section 3. In Section 4, a method of data fusion will be given step by step. Besides collecting all data and fuse them together, we also develop a standard to judge whether it is necessary to transmit and receive data. That standard will be talked about in Section 5. However, there is still some future work needed to research further, see Section 6. Then we give a conclusion in Section 7.

2. Introduction of Data Fusion in Leach

In LEACH [2], data fusion only performs when the local sensors send their data to the cluster header; the cluster header collects all the data and combines several unreliable data measurements to produce a more accurate signal by enhancing the common signal and signal and reducing the uncorrelated noise.

The method used in LEACH is routing-driven. Routing schemes in LEACH focus on the route design without explicit consideration of the fusion process as an additional requirement. It assumes that data fusion can be done at any node without additional computation cost and that full aggregation is achievable. Its goal is thus to minimize the total communication cost for gathering the data to the sink. Aggregation only occurs opportunistically when routes intersect. For example, in Figure 1, if both nodes A and B employ node E as their next hop for data routing purpose, their data will simply be fused at node E.

3. Fcm Algorithm

In order to improve the efficiency of LEACH, we use FCM [3] algorithm to do association in cluster headers.

If it is the first time then we choose One-step Delay Algorithm to start track, or else we choose FCM Algorithm to fuse data. The purpose of the algorithm is to classify the data into a number of known clusters. The clustering algorithms produce a degree of relationship between each data point to each cluster.

The aim function defined as follows:

$$J_m(U,E)=\sum_{k=1}^{n}\sum_{i=1}^{c}(u_{ik})^m d_{ik}, \tag{1}$$

$$d_{ik}=\|s_k-e_i\|^2. \tag{2}$$

where m is a real number belong to $[1,\infty)$ called the fuzzification constant. s_k is the k^{th} data sample and e_i is the i^{th} cluster. The goal of the algorithm is to determine the optimum degrees of membership, and the optimum fuzzy cluster centers e_i , so that the sum of the square errors J_m is minimum.

$$U_{ik}=\frac{1}{\sum_{j=1}^{c}(\frac{d_{ik}}{d_{jk}})^{\frac{2}{m-1}}}\forall i,k, \tag{3}$$

$$e_i=\frac{\sum_{k=1}^{n}(u_{ik})^{m_{S_k}}}{\sum_{k=1}^{n}(u_{ik})^m}\forall i, \tag{4}$$

4. Application of Fcm Algorithm for Data Fusion

Now, let us focus on how to apply FCM Algorithm. Assume sensor network is like Figure 2, we should define $E=\{e_1,e_2,...,e_c\}$ as the set of estimating positions of the sensed tracks and $S=\{s_1,s_2,...,s_n\}$ is the set of sensed data in one gathering circuit.

In order not to miss nodes and not to link too faraway nodes like Figure 3, the steps of association are as follows [4]:

I. Estimate data of formed tracks;

II. each track has an estimated position and estimated velocity. Make a circle around the estimated position of each track within a radius of maximum velocity multiply the gathering cycle. That is the limit region;

III. Disperse all the received data points into all the limit regions. Define the aggregates of the data as S_a, S_b and S_c, $S_a\bigcup S_b\bigcup S_c\subseteq S$;

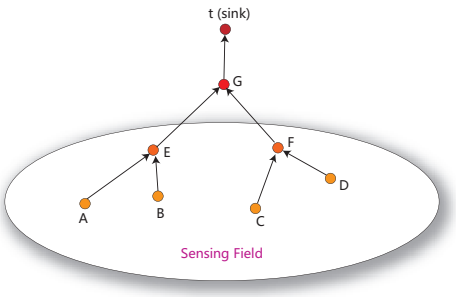

Figure 1. Routing-driven data fusion

IV. Calculate the relationship between element $i \in E$ and all the elements in S_i; Assign the maximum associated data points to each track. It can follow from below:
   (a) Build up a matrix of the relationship between E and S. Define the relationship as $u(e_i, s_k)$, $e_i \in E$, $s_k \in S_i$.
   (b) While the matrix is found, search for the maximum $u(e_m, s_n)$, and sign the sensed data s_n to estimated point e_m.
   (c) Expunction the m^{th} row and the n^{th} column.
   (d) Repeat step (b) and (c), till all the elements in E has been assigned.

V. If there is no data point in the limit region of track A, the evaluate data is given to the track A instead of sensed data.

You can understand the steps better by Figure 3.

5. Reduction of Transmitting Unchanged Data

When the clusters are ready, every cluster node starts to send data to its cluster head. There is a problem that when the node can send data for the second time. If the data keeps unchanged, the node still keeps sending it to the cluster head, which may cause the waste of energy. One way to improve this problem is as followings.

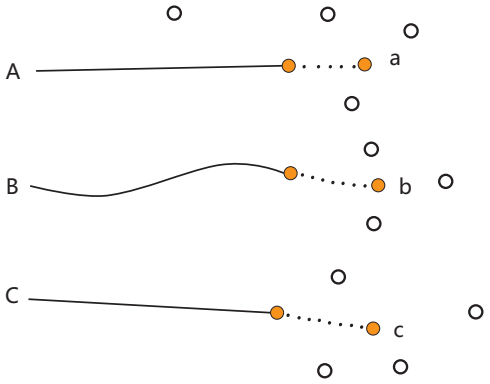

Figure 2. Sensor networking

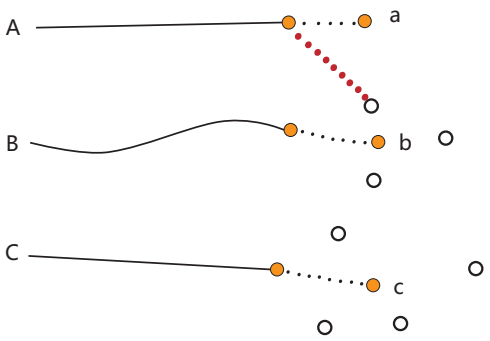

Figure 3. Faraway association

After each cluster head is decided, it can send both an absolute threshold and a comparative threshold to each node in its cluster. When a node receives data, firstly, it can compare it with the absolute threshold. If the data is larger, the node will send it to the cluster head and remember it. Then when the node receives another data, it will make a subtraction between the former record and the data and compare the result with the comparative threshold. The node won't send the data to the cluster head until the result is larger. And then the node will remember this new data.

The advantages are as follows:

I. It can make a quick reaction to the accident;

II. Aiming at a lasting accident, it won't send the data to the cluster head until it assumes the new one is different from the former. In this way, much energy which may be consumed in the useless repeated transmission will be saved.

6. Future Work

After association between the formed track list and the gathered data, the Algorithm reserve all the remanent data to do another association, so targets were repeated tracked. Data in the same limit region is more likely from the same target, just like the Figure 5. So a compromise solution is to delete the data in all the limit regions. The remanent data will take the second association. Then new targets are preserved and redundant data are deleted. However, better means remain under research.

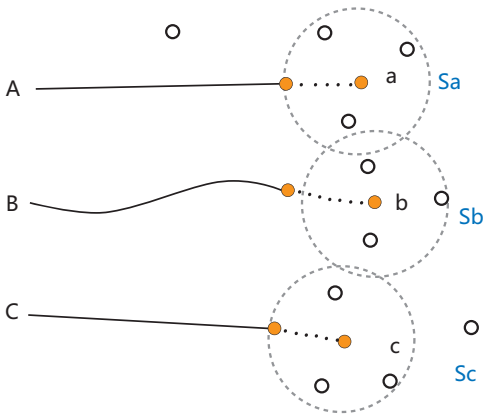

Figure 4. Application of FCM Algorithm

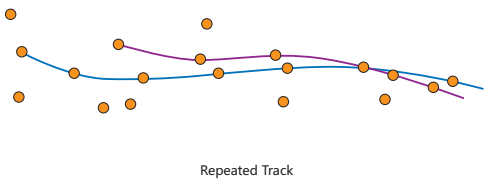

Figure 5. Repeated tracking

7. Conclusion

In this Chapter, we discuss about data fusion. Routing schemes supporting data fusion in wireless sensor networks can be classified into three categories: routing-driven, coding-driven, and fusion-driven [5]. LEACH belongs to the first kind.The most important metric of performance of a routing scheme supporting data fusion,is perhaps energy efficiency.

We give a brief introduction of FCM Algorithm and apply it as a data fusion method. That method is efficient and not complex. Besides, we talks another method to reduce unchanged or little changed data transmission. Our ongoing work is to improve our methods further and simulate them.

References

1. Wald, L., "A European proposal far terms of reference in data fusion", Intemational Archives of Photogrammetry and Remote Sensing, Vo.. XXXII, Part 7,pp.651-654,1998.
2. W. B. Heinzelman, A.P. Chandrakasan, and H. Balakrishnan, "Energy Efficient Communication Protocol for Wireless Microsensor Networks", Proceedings of 33rd Hawaii Int'l. Conf. Sys. Sci, 2000.
3. Ashraf Mamdouh Abdel-Aziz, Egyptian Armed Forces, "An All-Neighbor Fuzzy Association Approach In Multisensor-Multitarget Tracking Systems", 2lSt National Radio Science Conference (NRSC2004).
4. Lin Fan , Huanzhao Wang , Hai Wang, "A solution of multi-target tracking based on FCM Algorithm in WSN", Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW06).
5. Hong Luo,Yonghe Liu and Sajal K. Das, "Routing Correlated Data in Wireless Sensor Networks: A Survey", IEEE Network November/December 2007.

Part Three

SECURITY IN LEACH-LIKE WIRELESS SENSOR NETWORK ROUTING PROTOCOLS

XU MIAO

1. Introduction

Sensor networks are key to the creation of smart spaces, which embed information technology in everyday home and environment. The privacy and security issues posed by sensor networks represent a rich field of research problems. Every sensor network may consist of hundreds of thousands of sensor nodes and each node represents a potential point of attack, making it impractical to monitor and protect each individual sensor from either physical or logical attack. As a robust protocol, the security should be taken into consideration.

In the section two, we will give a whole description of the attackers, including different ways in which they can attack and the classification [1][2]. Then, we will discuss three kinds of attacks in details, focusing on energy attack in the third section [3]. At last, some countermeasures will be brought about [2].

2. Overview of Attacks

In wireless sensor network communications, all these protocols involve some forms of coordination and message exchanges between neighboring nodes in order to elect coordinators and determine sleep schedules. This protocols were designed assuming a non-adversarial trusted environment. Consequently, they are vulnerable to security attacks in some ways as follows:

I. attackers can capture and reprogram individual sensor nodes.
II. attackers can obtain their own commodity sensor nodes and induce the network to accept them as legitimate nodes, or they can claim multiple identities for an altered node.
III. attackers can do damage to the complete of the data, so that the receiver fails to acknowledge the information correctly.

Although attackers can make it in various ways, we can make a simple classification according to their roles played in a communication system.

Laptop-class vs node-class attackers [2]*:* A laptop-class attackers uses a relatively powerful device in comparison to a sensor node. An attacker with these capabilities has access to greater battery, storage and computational resources than a typical sensor node. It may also use high-power radio transmitter and every sensitive antenna that might allow the attacker to eavesdrop on the entire network, and transmit messages with enough power to be heard by any node. In contrast, a node-class attacker uses one or more devices with the same capabilities as legitimate sensor nodes. Therefore, it is able to listen to or transmit messages only within a

limited range, and it faces constraints such as limited battery power, small memory and a relatively slow CPU.

Outsider vs insider attackers [2]: An outsider attacker has no more knowledge than the definition of the protocols used in the network and the information gathered by eavesdropping on network communications. It has no access to cryptographic keys or data used to secure the network. For example, it does not possess any credentials that enable it to authenticate itself to other nodes. In contrast, an insider is an attacker that has all the information used by a node to be a legitimate member of the network, such as its cryptographic keys. It can be captured node, but also a device, such a node-class or laptop-class, in which the attacker has stored information retrieved from a compromised node. More insidious attackers can occur from inside the sensor network if attackers can compromise the sensor nodes. For example, they could create routing loops that will eventually exhaust all nodes in the loop.

3. Three Kinds of Attacks

As we all know, leach is a clustering-based protocol that utilizes randomized rotation of local cluster base stations to evenly distribute the energy load among the sensors in the network. From the decision of each cluster head to the data transmission, energy is the only standard. So we are ready to discuss three kinds of energy attacks.

I. because the nodes organize themselves into local clusters only according to the energy they receive, the attackers with evil intentions will easily attack this protocol by HELLO flooding [3]. For example, the attacker transmits data with so high energy that the nodes make a mistake to join this cluster. When a large amount of nodes belong to this cluster, the attacker will transmit the wrong data or rewrite the data. As a result, the useful data cannot be transmitted efficiently and the network is lost in confusion.

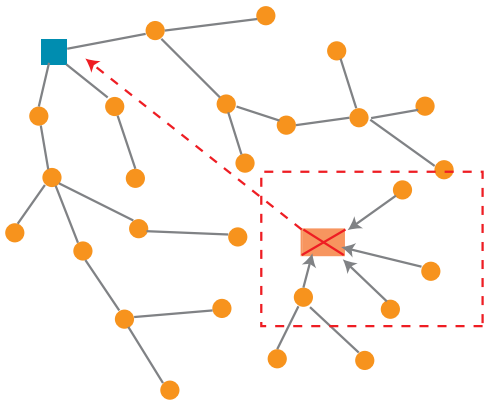

Figure 1. A network attacked by HELLO flooding

II. the attackers can occur at the physical layer. For example, via radio jamming [1]. They can also involve malicious transmissions into the network

to interfere with sensor network protocols or physically destroy central network nodes. Attackers can induce battery exhaustion in sensor nodes–for example, by sending a sustained series of useless communications that the targeted nodes will expend energy processing and may also forward to other nodes.

III. for the directly processing protocol, which is based on data, attackers can not prevent the base stations from broadcasting information directly, but it can create the false information via overhearing, exchanging with evil intentions the information and so on [3]. Just as the picture showed below, the attacker changes the routing of the information from N1 to N2, making the messages transmitted through the attacker itself, so it can do any exchange to the data at its own will.

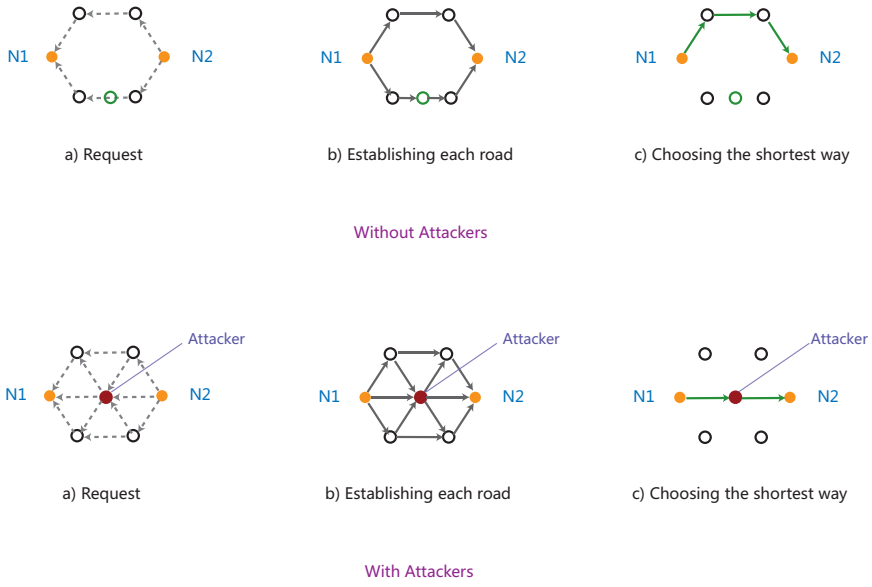

FIGURE 2. A network attacked by routing information tampering

4. COUNTERMEASURES

Potential defenses against denial-of-service attacks are as varied as the attacks themselves. Techniques such as spread-spectrum communication or frequency hopping can counteract jamming attacks. Proper authentication can prevent injected messages from being accepted by the network. However, the protocols involved must be efficient so that they themselves do not become targets for an energy-exhaustion attack. For example, using signatures based on asymmetric cryptography can provide message authentication. However, the creation and verification of asymmetric signatures are highly computationally intensive, and attackers that can induce a large number of these operations can mount an effective energy-exhaustion attack. The most important countermeasure against the attacks is to ensure that all communication between nodes is authenticated. Thus, sometimes efficient authentication mechanisms are also needed for local broadcast messages.

I. add coding to the data transmitted in a area. Any node can not change or rewrite the data if it doesn't have the code accordingly. But this method will lose effect on some insidious attackers.

II. metrics used by the protocol such as the node density should be computed based on estimates provided by multiple nodes in order to be robust to false estimates supplied by a malicious node. Each node uses a sequence number window that defines the interval of sequence numbers accepted [2]. This prevents attacker acting as a node from accepting the message. But this method will increase the complexity of the sensor network. Sometimes, there are some nodes died or some new nodes, each node will consume extra energy to change its own memory of sequence numbers.

5. Conclusion

In this section, we have analyzed the security vulnerabilities of protocols for wireless sensor networks, especially the leach-like protocols. Descriptions of common characteristics shared by attackers and classification of attacks give us a comprehensive view about attacks in wireless communications. In succession, we discuss, in details, three kinds of attacks maybe up against Leach, and accordingly, some countermeasures have been involved.

References

1. Haowen Chan and Adrian Perrig, "*Security and Privacy in Sensor Networks*," 2003.
2. Andrea Gabrielli, Luigi V.Mancini, Sanjeev Setia and Sushil Jajodia, "*Security Topology Maintenance Protocols for Sensor Networks: Attacks and Coun- termeassures*," IEEE, 2005.
3. Peng Jing, Zhai Ying, Liu Dongqing and Jiang Hong, "*Study on security of routing protocols in wireless sensor network*," 2006.