Study of Energy Efficient Wireless Sensor Network Protocols

S.Y.Amdani

Abstract : Wireless Sensor Networks are networks of large number of tiny, battery powered sensor nodes having limited on-board storage, processing, and radio capabilities. Nodes sense and send their reports toward a processing center which is called sink or base station. Since this transmission and reception process consumes lots of energy as compare to data processing, Designing protocols and applications for such networks has to be energy aware in order to prolong the lifetime of the network. Generally, real life applications deal with Heterogeneity rather than Homogeneity. In this paper, a protocol is proposed, which is heterogeneous in energy. We first completely analyze the basic distributed clustering routing protocol LEACH (Low Energy Adaptive Clustering Hierarchy), and SPIN focused on energy consumption.

Keywords - Security Protocols, Network Security, Energy efficient, Authentication, Wireless Sensor Networks

I. INTRODUCTION

WSNs usually consist of thousands of sensor nodes,and are deployed for a wide variety of applications, including military sensing and tracking, environment monitoring, patient monitoring, etc. When sensor networks are deployed in a hostile environment, security becomes extremely important [1]. The adversaries easily listen to the traffic, impersonate one of the nodes, or intentionally provide malicious information to other nodes. Security mechanisms that provide confidentiality and authentication are critical for the operation of many sensor applications. For this reason, variety protocols have been develped to provide confidentiality and authentication. WSNs are a special type of network which has many constraints such as limited power supplies, low bandwidth, and small memory size. The limited energy at senor nodes creates hindrances in implementing complex security schemes. There are two major factors for energy consumption:

1. Transmission and reception of data.
2. Processing of query request.

Wireless networks are relatively more vulnerable to security attacks than wired networks due to the broadcast nature of communication [1]. In order to implement security mechanism in sensor networks, we need to ensure that communication overhead is less and consumes less computation power. With these constraints it is impractical to use traditional security algorithms and mechanism meant for powerful workstations. Sensor networks are vulnerable to a variety of security threats such as DoS, eavesdropping, message replay, message modification, malicious code, etc. In order to secure sensor networks against these attacks, we need to implement message confidentiality, authentication, message integrity, intrusion detection and some other security mechanism.

Manuscript Received on March, 2014.

Dr. S.Y.Amdani, Associate Professor & Head Babasaheb Naik College of Engg, Pusad (Computer Science & Engineering, Babasaheb Naik College of Engg. Pusad, Amravati University, India.

Encrypting communication between sensor nodes can partially solve the problems but it requires a robust key exchange and distribution scheme. In general, there are three types of key management schemes [2,3]: Trusted Server scheme, self enforcing scheme and key predistribution scheme. Trusted server schemes relies on a trusted base station, that is responsible for establishing the key agreement between two communicating nodes as described in [4]. It uses symmetric key cryptography for data encryption. The main advantages of this scheme are, it is memory efficient, nodes only need to store single secret key and it is resilient to node capture. But the drawback of this scheme is that it is energy expensive, it requires extra routing overhead in the sense that each node need to communicate with base station several times [3]. Self enforcing schemes use public key cryptography for communication between sensor nodes. This scheme is perfectly resilient against node capture and it is fully scalable and memory efficient. But the problem with the traditional public keys cryptography schemes such as DSA [5] or RSA [6] is the fact that they require complex and intensive computations which is not possible to perform by sensor node having limited computation power. Some researchers [7,8] uses Elliptic curve cryptography as an alternative to traditional public key systems but still not perfect for sensor networks. Third scheme is key pre-distribution scheme based on symmetric key cryptography, in which limited numbers of keys are stored on each sensor node prior to their deployment. This scheme is easy to implement and does not introduce any additional routing overhead for key exchange. The degree of resiliency of node capture is dependent on the pre-distribution scheme [3]. Quite recently some security solutions have been proposed in [9,10,11,12,13] especially for wireless sensor networks but each suffers from various limitations such as higher memory and power consumptions.

Security Issues in WSN

- Key Management
  Encryption technologies are used to achieve secret communications to provide security. In order to encrypt the data, secret keys should be set up among communicating sensor nodes. Sensor nodes have limited computing power, making public key cryptographic primitives too expensive in terms of system overhead.
- Cryptography and Authentication
  In many applications, nodes communicate highly sensitive data. Therefore, WSNs need cryptography and authentication protocols as protection against eavesdrop-ping, injection, and modification of packets.
- Privacy
  WSNs are deployed in any place such as buildings, markets, and public places. For this

reason, individual information can be easily exposed to an adversary.

- Attack
  WSNs are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, WSNs have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected.

II. WSN PROTOCOLS

LEACH (Low Energy Adaptive Clustering Hierarchy) is designed for sensor networks where an end-user wants to remotely monitor the environment. In such a situation, the data from the individual nodes must be sent to a central base station, often located far from the sensor network, through which the end-user can access the data. There are several desirable properties for protocols on these networks:

- Use 100's - 1000's of nodes
- Maximize system lifetime
- Maximize network coverage
- Use uniform, battery-operated nodes

Conventional network protocols, such as direct transmission, minimum transmission energy, multi-hop routing, and clustering all have drawbacks that don't allow them to achieve all the desirable properties. LEACH includes distributed cluster formation, local processing to reduce global communication, and randomized rotation of the cluster-heads. Together, these features allow LEACH to achieve the desired properties. Initial simulations show that LEACH is an energy-efficient protocol that extends system lifetime. LEACH randomly selects a few sensor nodes as cluster heads (CHs) and rotates this role to evenly distribute the energy load among the sensors in the network. The idea is to form clusters of the sensor nodes based on the received signal strength and use local cluster heads as routers to the sink. In LEACH, the Cluster Heads compress data arriving from member nodes and send an aggregated packet to the BS in order to reduce the amount of information that must be transmitted to the BS. In order to reduce inter & intra cluster interference LEACH uses a TDMA/code-division multiple access (CDMA) MAC. The operation of LEACH is done into two steps, the setup phase and the steady state phase. In setup phase the nodes are organized into clusters and CHs are selected. These cluster heads change randomly over time in order to balance the energy of the network. This is done by choosing a random number between 0 and 1. The node is selected as a cluster head for the current round if the random number is less than the threshold value T (n), which is given by

$$T(n) = \begin{cases} \dfrac{p}{1 - p*(r \bmod \frac{1}{p})} & \text{if n } \varepsilon \text{ G} \\ 0 & \text{otherwise 0} \end{cases}$$

Here G is the set of nodes that are involved in the CH election. LEACH clustering is shown in Fig 1. In the steady state phase, the actual data is transferred to the BS. To minimize overhead the duration of the steady state phase should be longer than the duration of the setup phase. The CH node, after receiving all the data from its member nodes, performs aggregation before sending it to the BS. After a certain time period, the setup phase is restarted and new CHs is selected. Each cluster communicates using different CDMA codes to reduce interference from nodes belonging to other clusters.

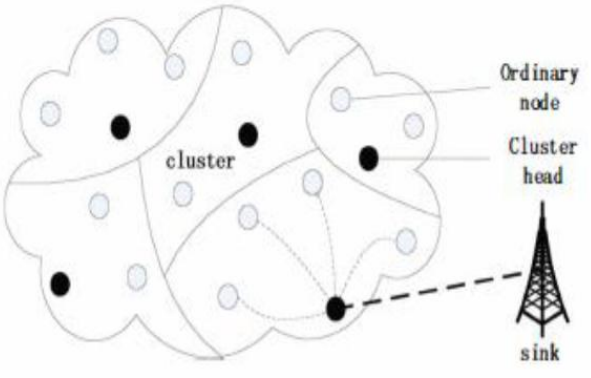

Fig 1 LEACH Protocol

LEACH achieves over a factor of 7x and 8x reduction in energy dissipation compared to direct communication and a factor of 4x and 8x compared to the minimum transmission energy (MTE) routing protocol. The major characteristics of this Protocol are as follow: The cluster heads are rotated in a randomized fashion to achieve balanced energy consumption. It is assumed that all the sensors have synchronized clocks so that they know the beginning of a new cycle. In LEACH sensors do not need to know location or distance information. There are some drawbacks associated with this protocol such as: Single-hop routing is used where each node can transmit directly to the cluster-head and the sink. CHs are elected randomly; hence there is Possibility that all CHs will be concentrated in same area. The idea of dynamic clustering is used which leads to extra overhead due to cluster head changes, advertisements etc. The protocol assumes that all nodes are having same amount of energy. It also assumes that CH consumes approximately the same amount of energy for each node SPIN (Sensor Protocols for Information via Negotiation) Sensor Protocols for Information via Negotiation (SPIN) that disseminates all the information at each node to every node in the network assuming that all nodes in the network are potential BSs. This enables a user to query any node and get the required information immediately. These protocols make use of the property that nodes in close proximity have similar data, and hence there is a need to only distribute the data other nodes do not posses. The SPIN family of protocols uses data negotiation and resource-adaptive algorithms. Nodes running SPIN assign a high-level name to completely describe their collected data (called meta-data) and perform metadata negotiations before any data is transmitted. This ensures that there is no redundant data sent throughout the network. The semantics of the meta-data format is application-specific and not specified in SPIN. For example, sensors might use their unique IDs to report meta-data if they cover a certain known region. In addition, SPIN[5] has access to the current energy level of the node and adapts the protocol it is running based on how much energy is remaining. These protocols work in a time-driven fashion and distribute the information all over the network, even when a user does not request any data. The SPIN family is designed to address the deficiencies of classic flooding by negotiation and resource adaptation. The SPIN family of protocols is designed based on two basic ideas:

1) Sensor nodes operate more efficiently and conserve energy by sending data that describe the sensor

data instead of sending all the data; for example, image and sensor nodes must monitor the changes in their energy resources.

2) Conventional protocols like flooding or gossiping-based routing protocols [2] waste energy and bandwidth when sending extra and unnecessary copies of data by sensors covering overlapping areas.

SPIN's meta-data negotiation solves the classic problems of flooding, thus achieving a lot of energy efficiency. SPIN is a three-stage protocol as sensor nodes use three types of messages, ADV, REQ, and DATA, to communicate. ADV is used to advertise new data, REQ to request data, and DATA is the actual message itself. The protocol starts when a SPIN node obtains new data it is willing to share. It does so by broadcasting an ADV message containing metadata. If a neighbor is interested in the data, it sends a REQ message for the DATA and the DATA is sent to this neighbor node. The neighbor sensor node then repeats this process with its neighbors. As a result, the entire sensor area will receive a copy of the data. The SPIN family of protocols includes many protocols. The main two are called SPIN-1 and SPIN-2; they incorporate negotiation before transmitting data in order to ensure that only useful information will be transferred. Also, each node has its own resource manager that keeps track of resource consumption and is polled by the nodes before data transmission. The SPIN-1 protocol is a three-stage protocol, as described above. An extension to SPIN-1 is SPIN-2, which incorporates a threshold-based resource awareness mechanism in addition to negotiation. When energy in the nodes is abundant, SPIN-2 communicates using the three-stage protocol of SPIN1. However, when the energy in a node starts approaching a low threshold, it reduces its participation in the protocol; that is, it participates only when it believes it can complete all the other stages of the protocol without going below the low energy threshold. In conclusion, SPIN-1 and SPIN-2 are simple protocols that efficiently disseminate data while maintaining no per-neighbor state. These protocols are well suited to an environment where the sensors are mobile because they base their forwarding decisions on local neighborhood information. One of the advantages of SPIN is that topological changes are localized since each node need know only its single-hop neighbors. SPIN provides more energy savings than flooding, and metadata negotiation almost halves the redundant data. However, SPIN's data advertisement mechanism cannot guarantee delivery of data. To see this, consider the application of intrusion detection where data should be reliably reported over periodic intervals, and assume that nodes interested in the data are located far away from the source node, and the nodes between source and destination nodes are not interested in that data; such data will not be delivered to the destination at all.

Table1. Comparison between LEACH and SPIN Protocol

	LEACH PROTOCOL	SPIN PROTOCOL
Classification	Hierarchical	Flat
Mobility	Fixed BS	Poss.
Position Awareness	No	No
Power usage	Max	Ltd
Negotiation Based	No	Yes
Data Aggregation	Yes	Yes
Localization	Yes	No
Query Based	No	Yes
State Complexity	CHs	Low
Scalability	Good	Limited
Multipath	No	Yes

III. CONCLUSION

Routing protocols designed for WSNs should be as energy efficient as possible to prolong the lifetime of individual sensors, and hence the network's lifetime. In this paper we have surveyed LEACH and SPIN protocols and discussed how they improve energy consumption in WSNs and increase network's lifetime. Furthermore, we provide a table summary showing their comparison.

REFERENCES

1. J.P. Walters, Z. Liang, W. Shi, and V. Chaudhary,"Wireless Sensor Network Security: A Survey," TechnicalReport MIST-TR-2005-007, July, 2005.
2. J.P. Walters, Zh. Liang, W. Shi, V. Chaudhary, Security in Distributed, Grid, and Pervasive Computing, Chapter 17, CRC Press, 2006.
3. A. Perrig, R. Szewczk, J.D. Tygar, V. Wen, D.E. Culler, SPINS: Security Protocols for Sensor Networks, Wireless Networking, Vol. 8, No. 5, pp. 521-534, Sept 2002.
4. A. Perrig, R. Canneti, J. D. Tygar, D. Song, The TESLA Broadcast Authentication Protocol, Crypto Bytes, Vol. 5, No. 2, pp. 2-13, 2002.
5. D. Boyle, T. Newe, Security Protocols for use with Wireless Sensor Networks: A Survey of Security Architectures, Proceedings of the 3rd International Conference on Wireless and Mobile Communications, Guadeloupe, French Caribbean, pp. 54, 04-09 March 2007.
6. Sun Limin, Li Jianzhong, Chen Yu, ―Wireless Sensor Networks, Tsinghua publishing company Beijing, 2005.
7. Wendi Rabiner, Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan, Energy-efficient Communication Protocol for Wireless MicrosensorNetworks, In: Proc. of 33rd Annual Hawaii Inter Cord on System Sciences, Hawaii, USA: IEEE Computer Society, 2000.
8. Li Han, LEACH-HPR: An Energy Efficient Routing Algorithm for heterogeneous WSN IEEE 2010.
9. Vivek Mhatre and Catherine Rosenberg, Homogeneous Vs Heterogeneous Clustered Sensor Networks:A Comparative Study In Proceeding of IEEE International Conference on Communications(ICC), 2004, PP. 3646-3651.
10. Georgious Smaragdakis, Ibrahim Matta and Azer Bestavors, ―SEP: A Stable Election Protocol for Clustered Heterogeneous Wireless Sensor Networks. In Proceding of the International Workshop on SANPA, 2004.
11. Wendi Rabiner Heinzelman, Amit Sinha. Alice Wang and Anatha P. Chandrakasan, ―Energy Scalabel Algorithms and Protocols for Wireless Micro sensor Networks, 2000.
12. J. Al-Karaki, and A. Kamal, Routing Techniques in Wireless Sensor Networks: A Survey., IEEE Commun-ications Magazine, vol 11, no. 6, Dec. 2004, pp. 6-28.
13. W.R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, An Application-Specific Protocol Architecture for Wireless Microsensor Networks. In IEEE Transactions on Wireless Communications vol. 1(4), 2002, pp. 660-670.
14. Yan Li, Yan Zhong Li, Energy-Efficient clustering Routing algorithm based on LEACH, Journal of Computer Applications, 2007.
15. Ben Alla Said, Ezzati Abdellah, Abderrahim Beni Hssane, Moulay Lahcen Hasnaoui, ―Improved and Balanced LEACH for heterogeneous wireless sensor networks (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 08, 2010, 2633-2640
16. Zeenat Rehena, Sarbani Roy, Nandini Mukherjee ,"A Modified SPIN for Wireless Sensor Networks", 978-1-4244 8953-4/11 2011 IEEE.