BIOINFO Sensor Networks
ISSN: 2249-944X & E-ISSN: 2249-9458 Volume 2, Issue 1, 2012, pp.-25-29.
Available online at http://www.bioinfo.in/contents.php?id=301

PROVIDING END-TO-END SECURE COMMUNICATION USING KEY MANAGEMENT TECHNIQUE IN WIRELESS SENSOR NETWORK

ANIKET JUNGHARE[1] AND ABHIJEET BAGADI[2]

[1]MIT, Pune, MS, India.
[2]MITCOE, Pune, MS, India.
*Corresponding Author: Email- aniket5junghare@gmail.com

Received: February 21, 2012; Accepted: March 15, 2012

Abstract- In many Wireless Sensor Networks (WSNs), providing end to end secure communications between sensors and the sink is important for secure network management. While there have been many works devoted to hop by hop secure communications, the issue of end to end secure communications is largely ignored. This introduce design an end to end secure communication protocol in randomly deployed WSNs. Specifically, the protocol is based on a methodology called differentiated key pre-distribution. The core idea is to distribute different number of keys to different sensors to enhance the resilience of certain links. This feature is leveraged during routing, where nodes route through those links with higher resilience. Using rigorous theoretical analysis, an expression for the quality of end to end secure communications is derive, and use it to determine optimum protocol parameters. Extensive performance evaluation illustrates that this solutions can provide highly secure communications between sensor nodes and the sink in randomly deployed WSNs. Also provide detailed discussion on a potential attack (i.e. biased node capturing attack) to the solutions, and propose several countermeasures to this attack. .
Keywords- Sensor networks, security, key management, Routing Protocols

Citation: Aniket Junghare and Abhijeet Bagadi (2012) Providing End-To-End Secure Communication Using Key Management Technique in Wireless Sensor Network. BIOINFO Sensor Networks, ISSN: 2249-944X & E-ISSN: 2249-9458 Volume 2, Issue 1, pp.-25-29.

Introduction

A wireless sensor network (wsn) is a wireless network consisting of a large number of spatially distributed sensor nodes. These sensor nodes can be easily deployed at strategic regions at a low cost. Equipped with various types of sensors, sensor nodes cooperate with each other to monitor physical or environmental conditions, such as temperature, sound, image, vibration, pressure, motion or pollutants. Each sensor node is also equipped with a radio transceiver or other wireless communication device, a microprocessor, and an energy source (e.g., a battery). Due to cost and size constraints, sensor nodes are usually resource limited with respect to their energy, memory, computational, and communication capacities. The development of WSNS was originally motivated by military and homeland security applications such as battlefield surveillance. However, WSNS are now also widely applied in civilian application areas, including industrial sensing, environment and habitat monitoring, health-care applications, home automation, and traffic control. In the context of ubiquitous computing, WSNS can be used to perform ubiquitous information sensing, storing, and provide content delivering services. Due to their broad applications in both military and civilian domains, WSNS have drawn a lot of attention recently. Communication security is essential to the success of WSN applications, especially for those mission-critical applications working in unattended and even hostile environments.

Key Management Schemes In Sensor Networks

Numerous key management schemes have been proposed for sensor networks. The objective of key management is to dynamically establish and maintain secure channels among communicating nodes. Many schemes, referred to as static schemes, have adopted the principle of key predistribution with the underlying assumption of a relatively static short-lived network (node replenishments are rare, and keys outlive the network). An emerging class of schemes, dynamic key management schemes, assumes long-lived networks with more frequent addition of new nodes,

thus requiring network rekeying for sustained security and survivability.

The success of a key management scheme is determined in part by its ability to efficiently survive attacks on highly vulnerable and resource challenged sensor networks. Key management schemes in sensor networks can be classified broadly into dynamic or static solutions based on whether rekeying (update) of administrative keys is enabled post network deployment.

1) Static Key Management Schemes

The static schemes assume that once administrative keys are predeployed in the nodes, they will not be changed. Administrative keys are generated prior to deployment, assigned to nodes either randomly or based on some deployment information, and then distributed to nodes. For communication key management, most static schemes use the overlapping of administrative keys to determine the eligibility of neighboring nodes to generate a direct pair-wise communication key. Communication keys are assigned to links rather than nodes. In order to establish and distribute a communication key between two non neighboring nodes and/or a group of nodes, that key is propagated one link at a time using previously established direct communication keys.

2) Dynamic Key Management Schemes

Dynamic key management schemes may change administrative keys periodically, on demand or on detection of node capture. The major advantage of dynamic keying is enhanced network survivability, since any captured key(s) is replaced in a timely manner in a process known as rekeying. Another advantage of dynamic keying is providing better support for network expansion, upon adding new nodes, unlike static keying, which uses a fixed pool of keys, the probability of network capture increase is prevented. The major challenge in dynamic keying is to design a secure yet efficient rekeying mechanism. A proposed solution to this problem is using exclusion-based systems (EBSs); a combinatorial formulation of the group key management problem.

Conceptual Theory of WSN Security

In many applications under hostile environment, sensor nodes cannot be deployed deterministically and thus are randomly deployed into the field. An important requirement in network management of many mission critical applications is to secure end to end sensor networks data from being eavesdropped by the attacker. There exist two intuitive approaches to provide a high degree of end to end secure communications in WSNs:

1. The first one is distributing a unique pair-wise key into each sensor and the sink prior to deployment, and letting each sensor use this pair-wise key to encrypt the communications with the sink.
2. The second one is simply providing hop by hop secure communications between neighboring sensors in the network. It is in general believed that in this way end to end secure communications can naturally be achieved via hop by hop encryption/ decryption.

The first approach has critical limitations in multi-hop WSNs since it precludes the possibility of intermediate sensors performing encryption/decryption along the path. This feature is necessary for interpreting and aggregating data at intermediate sensors to save energy (a critical requirement in WSNs), authenticating received data to defend against fake packets injection attack, denial of service attack etc. Hence in WSNs, need to use hop by hop based encryption/decryption in providing end to end secure communications.

The second approach works well if all links in the network are highly resilient. However, it is very hard, if not impossible to achieve high resilience for all the links in randomly deployed WSNs. This is due to inherent resource limitation of sensor, nature of random deployment and presence of attacks. In fact, with random key pre-distribution (RKP) [2] based schemes, a majority of links in the network have low resilience under reasonable memory constraint and even under mild attack strength, which restricts room for providing a high degree of end to end secure communication.

The resilience of each hop (link) can be reflected by the number of shared pre-distributed keys in the link. It is known that under uniform key distribution, i.e. each sensor pre-distributed with equal number of keys, will achieve maximum average number of shared pre-distributed keys in each link. However, there is an inherent limitation in uniform key distribution as demonstrated in Fig.1 In Fig.1, Suppose we have 1000 nodes randomly deployed in a circular network with radius 500 , where = 40, = 10000 and communication range of each node is 100 . From this it's seen that a majority of links have low resilience (i.e., small number of shared keys), while the percentage of links that are highly resilient is quite low. This clearly restricts the room for routing protocols to choose more resilient links during end to end communications. Installing more keys into each node is not always preferable since it enables the attacker to disclose more keys upon node captures, which could again compromise the link resilience.

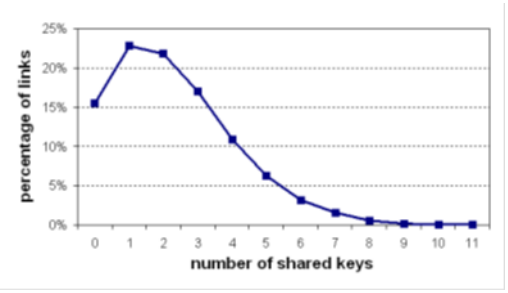

Fig. 1- Percentage of links with varying number of shared keys

Key Predistribution Schemes

A. RKP based schemes

There are of brief background on random key pre-distribution (RKP) schemes, attack models and performance metrics in randomly deployed WSNs.

1. Basic RKP scheme

A well accepted scheme for secure communications in randomly deployed WSNs is random key pre-distribution (RKP) where there are two stages. At the key pre-distribution stage, each node is pre-distributed with distinct keys randomly chosen from a large pool of keys, and then nodes are randomly deployed. At the pair-wise key establishment stage, each node first obtains its neighborhood information. If two neighbors share one or more pre-distributed keys, they establish a pair-wise key in between directly. To do so, one node can generate a random pairwise key and send it to its neighbor encrypted with their shared keys. For two neighbors that

do not share pre-distributed key, they will use neighboring nodes, called proxies, to construct key paths for pair-wise key establishment using above process.

2. Variants of (RKP) Scheme

Many variants have been proposed based on the above idea of key pre-distribution in WSNs, including for homogeneous sensor networks, heterogeneous sensor networks and also (more recently) mobile sensor networks.

Homogeneous sensor network: In homogeneous sensor networks, the number of keys distributed per node is the same, and the network topology is flat.

Heterogeneous sensor networks: A heterogeneous wireless sensor network (HWSN) is shown in Figure 4.1. From this figure, it is seen that there is a hierarchy among the nodes based on their capabilities: base station, cluster heads and sensor nodes.

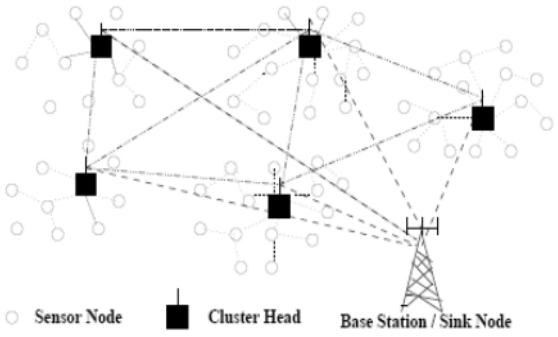

Fig. 2- A heterogeneous wireless sensor network (HWSN) architecture.

There are works on key management in heterogeneous sensor networks. cluster heads are distributed with more keys than normal sensors. However, in analysis of cluster heads are assumed to be equipped with a fast encryption/deletion algorithm to protect their supplementary keys from compromise. The keys are divided in different categories such as cluster key (shared among all members of the cluster), intermediate key (shared between a smaller subset of cluster members) and private key of each sensor (used to communicate with cluster head).

Mobile sensor networks: Mobile sensor networks have recently been studied in and there have been some recent efforts on key management on them. A pair-wise key management in sensor networks is proposed where sensors can move from one network to another Mobile wireless sensor networks have been shown to demonstrate enhanced performance over static wireless sensor networks. Because of the mobility of the sink, in general, much work can be shared by the mobile sink. Some of the advantages gained through mobile wireless sensor network over traditional sensor network are presented here with.

One major advantage of mobile WSN over static WSN is its efficient energy usage. In static WSN, the nodes closer to the gateway sink always lose their energy first, thus causing the overall network to "die". But in the case of mobile WSN, because of the mobility, sensor nodes' energy dissipation is more efficient.

Routing Protocol in WSN

Routing in wireless sensor networks has some differences from that in traditional wired and wireless ad hoc networks due to resource constraints, faults/failures etc. There are two main paradigms of routing protocols in WSNs: location-centric routing and data-centric routing.

A. Location-centric routing

Greedy Perimeter Stateless Routing (GPSR) is a well known location centric routing protocol. In GPSR, messages are broadcast by each node to inform its neighbors of its position. GPSR assumes that sensors can determine through separate means the location of the sink. Each node makes forwarding decisions based on the relative position of the sink and its neighbors. In general, the neighbor that is closest to the sink is chosen.

GPSR is a novel routing protocol for wireless datagram networks that uses the positions of routers and a packet's destination to make packet forwarding decisions. GPSR makes greedy forwarding decisions using only information about a router's immediate neighbors in the network topology. When a packet reaches a region where greedy forwarding is impossible, the algorithm recovers by routing around the perimeter of the region. By keeping state only about the local topology, GPSR scales better in per-router state than shortest-path and ad-hoc routing protocols as the number of network destinations increases. Under mobility's frequent topology changes, GPSR can use local topology information to find correct new routes quickly.

B. Data-centric routing

Directed diffusion is the most well known data centric routing protocol, in which the sink sends queries to all nodes and waits for data from the nodes satisfying specific requirement (e.g., located in selected regions, sensing data meet certain criteria, etc). In order to create a query, an interest is defined using a list of attribute value pairs such as name of objects, geographical area, etc. The interest is broadcast through the network, and used by each node to compare with the data received. The interest entry also contains several gradient fields. A gradient is a reply link to a neighbor from which the interest was received. By utilizing interests and gradients, paths are established between sensors and the sink. Several paths may be established, and one of them is selected by reinforcement.

Methodology of Providing End to End Secure Communication

In order to provide a high quality of end to end secure communications, it is clear that it should be enhance the resilience of individual links in the network. An intuitive way to do so is to increase the number of keys predistributed into each node (k). When the number of shared keys in each link increases, resilience seems to increase since all shared keys have to be disclosed to compromise the link.

A methodology called differentiated key pre-distribution is used to enhance the quality of end to end secure communications in randomly deployed WSNs. Methodology is based on the observation that links in the network are not equally important with respect to secure communications. Only the links used for data transmission have impacts on security. The core idea of our methodology is to pre-distribute different number of keys to different nodes. Keep the average number of keys per node the same as that in uniform key pre-distribution, so that the attacker impact(e.g., average number

of keys disclosed per node capture) remains the same. By distributing more keys to some nodes, the links between those nodes tend to have much higher resilience than the link resilience under uniform key predistribution. These high resilient links are preferred during routing to enhance the end to end secure communications.
This methodology can illustrate using the example in where 1000 sensors are deployed randomly in a WSN under the same scenario. Divide the 1000 nodes into two classes, with 200 nodes in the first class and 800 nodes in the second. Distribute k1 = 80 keys in each first class node and distribute k2 = 30 keys in each second class node. As such, the average number of keys per node is the same as where k is the same for all nodes.The impacts of this methodology. It shows that while applying differentiated key predistribution for the above setting, the number of high resilient links (those with large number of shared keys) dramatically increases, with the cost that the number of low resilience links also increases. This is because compared with the link resilience in traditional RKP schemes with uniform key pre-distribution, the links between two first class nodes in the scheme tend to have higher resilience, while those between two second class nodes tend to have relatively lower resilience. When those high resilient links are preferred during routing path selection, the end to end security performance can be enhanced significantly.

Biased Node Capturing Attack and Its Countermeasures
The attacker captures a certain percent of the nodes in the network. Such an attack is an unbiased one since the captured nodes are chosen at random. The type of advanced attack model, denoted as biased node capturing attack, in which the attacker has bias in choosing nodes to capture, aiming to achieve higher attack impact.

A. Biased Node Capturing Attack
Simply put, biased node capturing attack is one in which the attacker attempts to capture some special nodes in the network. Typically, the capture of those nodes results in higher attack impact, and they are chosen with bias instead of randomly. The existence of such special nodes comes from the fact that the roles (or importance) of sensor nodes in the network are inherently different. In a multi-hop sensor network, the nodes near the sink are such special nodes, whose capture results in more secret information disclosed to the attacker. This is because a node near the sink generally forwards more traffic, and its capture results in more data being disclosed. Thus, the attacker can take advantage of the heterogeneity in topology to capture those important nodes near the sink. In differentiated key management, also introduce a type of heterogeneity among the nodes in that different nodes have different number of pre-distributed keys. The capture of nodes with more pre-distributed keys tends to have higher attack impact due to the fact that more pre-distributed keys are disclosed. Thus, the attacker could also take advantage of the heterogeneity in the number of pre-distributed keys to achieve higher attack impact. Such an attack can be easily accomplished via identifying more resilient links (and hence nodes) via simple traffic analysis of monitored communication. Find that the biased attacks result in higher attack impact than unbiased one. However, the attack impact caused by biased attack based on topology alone is much more severe than that caused by biased attack based on key alone. Besides, the impact of the combined attack is close to that caused by the biased attack based on topology alone. This is because the nodes close to the sink are generally those forwarding more traffic. The capture of a few such nodes results in a significant portion of the data being disclosed.

B. Countermeasures
The biased attack based on topology naturally exists in multi-hop sensor networks, and thus is not introduced in differentiated key management. One potential countermeasure is letting the nodes near the sink just forward the encrypted data without needing to decrypt it for aggregation. In this way, the capture of such nodes does not disclose the data forwarded. To do so, nodes with a certain number of hops away from the sink need to be predistributed with a unique pair-wise key with the sink before node deployment. Such approach comes at the cost that no data aggregation is conducted near the sink. An alternative countermeasure is letting the sink node move around the network so the amount of forwarded traffic is balanced among the nodes in the network. Thus, the impact of such biased attack is alleviated.
The biased attack based on number of pre-distributed keys causes higher attack impact although such impact is far less than that of biased attack based on topology. One countermeasure is to use tamper resistant hardware for nodes pre-distributed with more keys. Therefore, such nodes become more robust to attack in that the attacker may not be able to obtain secret information in the captured node. Such idea is inspired by the work in where some special nodes are assumed never to disclose their secret information after capture. Such assumption is allowing a certain probability of secret information in such nodes being disclosed. The security performance of our differentiated key management under biased attack based on number of pre-distributed keys is better than that under unbiased attack the performance under biased attack falls below that under unbiased attack since more predistributed keys are disclosed. However, it is still better than that in traditional uniform key management.

Conclusion
The issue of providing end to end secure communications in randomly deployed wireless sensor networks is address, via differentiated key pre-distribution, where the idea is to distribute different number of keys to different sensors to enhance the resilience of certain links in the network. This feature is leveraged during routing, where nodes route through links with higher resilience. Using theoretical analysis an expression are derived for the quality of end to end secure communications and use it to determine optimum protocol parameters. End to end secure communication protocol based on the above methodology by extending well known location centric (GPSR) and data centric (minimum hop) routing protocols. Detailed theoretical analysis demonstrates the strengths of this technique.

Acknowledgement
Our thanks to the experts who have contributed towards survey of this paper.

References
[1] Gu W., Dutta N., Chellapan S., Bai X. (2011) *proc. IEEE conf.*
[2] Eschenauer L. and Gligor V.D. (2002) *9th ACM Conf. Comput. Commun. Security*.

[3] Chan H., Perrig A. and Song D. (2003) *Proc. IEEE Symp. Research Security Privacy*.
[4] Du W., Deng J., Han Y.S. and Varshney P.K. (2003) *Proc. 10th ACM Conf. Comput. Commun Security*.
[5] Liu D. and Ning P. (2003) *Proc. 10th ACM Conf. Comput. Commun. Security*.
[6] Traynor P., Choi H., Cao G., Zhu S. and Porta T. L. (2006) *Proc. 25th IEEE Conf. Comput. Commun*.
[7] Du W., Deng J., Han S., Chen S. and Varshney P. (2004) *23rd Annual Joint Conf. IEEE Comput. Commun. Societies*.
[8] Das A.K. (2011) *An Unconditonally Secure Key Management sceme for large-scale Heterogeneous Wireless Sensor Netwok- IIT Bhubaneshwar*.
[9] Karp B. and Kung H. (2000) *Proc. ACM International Conf. Mobile Comput. Netw*.
[10] Intanagonviwat C., Govindan R. and Estrin D. (2000) *Proc. ACM International Conf. Mobile Comput. Netw*.