International Journal of Computer Science and Engineering Research and Development (IJCSERD), ISSN 2248-9363 (Print), ISSN 2248-9371 (Online), Volume 1, Number 2, May-October (2011) pp. 28-36 © PRJ Publication http://www.prjpublication.com/IJCSERD.asp

IJCSERD

© PRJ PUBLICATION

INVESTIGATING SECURITY MECHANISMS IN WIRELESS SENSOR NETWORK

Madhuri Rao, K.Vinod Kumar, Laxmishree Panigrahi, Sharmista Kar and Subrat Kumar Nayak
Department of Computer Science and Engineering
S.O.A University, Bhubaneswar, Orissa 751030

ABSTRACT

Wireless sensor nodes are gaining huge popularity in many domains. This data acquisition system has tremendous significance in defense, traffic management and many more areas. Ensuring the security of both the collected data and the process of data collection is vital for the success of WSNs (Wireless Sensor Networks).Security is achieved when one is able to address all possible kinds of threat to the device and the technology standards including the software approach and cryptographic approach. Cryptographic means alone are not sufficient to mitigate attacks ,the use of statistics, data analysis and techniques from economics like game theory, ant colony optimization techniques could help .The communication of a wireless sensor network can be eavesdropped quite easily due to its properties, thereby requiring security mechanism here as well. Then stochastic routing is also designed to reduce the probability of successful prediction by a malicious node which is also a serious kind of security flaw. SPREAD used in MANETs, could be considered in case of WSNs too. We aim to discuss and survey some existing security measures like SPREAD, random key pre distribution mechanisms, Actuation environments and stochastic routing protocols for security. We conclude in a note suggesting, a mix of societal norms, new laws, and technological responses as being necessary to address security in WSN full fledge swing.

KEYWORDS: Wireless Sensor Network, Security, Network attacks, Key-Pre Distribution, SPREAD.

1. INTRODUCTION

Ensuring the security of both the collected data and the process of data collection is vital for the success of WSNs (Wireless Sensor Networks). Because of the constraints of the particular applications and the resource limitations, the security of WSNs is vastly different from that of conventional wired networks. For the example of military applications, wireless sensor nodes usually are sent to an unattended environment (e.g., the battlefield). In these scenarios, wireless sensor nodes are easier to capture or destroy.

Thus, the foremost important thing for WSNs is that they can tolerate the dysfunction of a certain number of nodes. The second possible attack for WSNs is that the enemy could distribute a certain number of faked sensor nodes to disturb or even disrupt the communications of legitimate sensors. It is important for a sensor network to design a security mechanism to protect the sensor nodes from malicious attack or to ensure that the sensor network can "tolerate" the malicious attack to some extent. Work in [1],[2],[3] have outlined and discussed such attacks .

The second challenge for the design of security mechanisms for WSNs is that sensor nodes are always equipped with limited battery and memory. Thus, the traditional public-key–based schemes, such as the Rivest–Shamir–Adleman (RSA) and Diffie–Hellman (D-H) protocols, are not suitable for WSNs. For example, Mica Mote, produced by UC Berkeley, has 128 kb Flash memory and 4 kb RAM. The WSN itself is not stable; e.g., the links could be on or off depending on the transmission environment, battery power of nodes, and the traffic load. This poses another challenge for the design of security mechanisms for WSNs compared with the wired networks. In this paper, current scenario of existing security measures is surveyed and summarized .Section 2 outlines the various layers of WSN and the kinds of attacks encountered. Existing WSN protocols and known relevant attacks are discussed in section here. Key Management schemes including the random key-pre-distribution ones are discussed in section 3. Stochastic routing protocols based on probability are outlined in section 4. SPREAD scheme is briefed in section 5.

2. LITERATURE REVIEW

Currently much of work is going on providing layered security for ex.- Holistic Security Approach, security is to be ensured for all the layers of the protocol stack as shown in fig1 and also cost of security should not be more than assessed security risks.

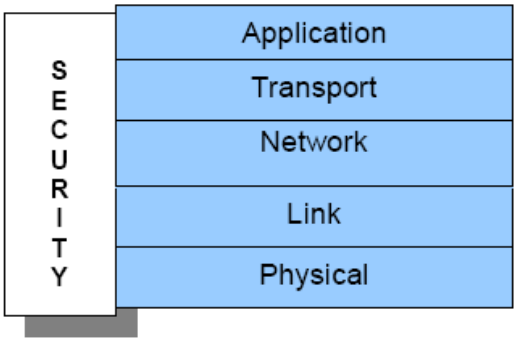

Fig 1: Holistic view of security

But major disadvantage with holistic security is that it is layered and tries to implement security mechanisms for each layer, which results in wastage of power, memory, processing power and introduce message delay. These WSN are susceptible to a variety of attacks, including node capture, physical tampering, and denial of service, while prompting a range of fundamental research challenges.

2.1 Categorization of network-layer attacks

As discussed in Karlof and Wagner (2003), most network-layer attacks against sensor networks fall into one of the following categories [5]: We have presented in Table 1some of the existing protocols with attacks that they are susceptible to.

Spoofed, altered, or replayed routing information : The most direct attack against a routing protocol is to target the routing information exchanged between nodes. By spoofing, altering, or replaying routing information, adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end-to-end latency, etc

Selective forwarding: Multihop networks are often based on the assumption that participating nodes will faithfully forward received messages. In a selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further. Selective forwarding attacks are typically most effective when the attacker is explicitly included on the path of a data flow.

Sinkhole attacks: In a sinkhole attack, the adversary's goal is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. Because nodes on, or near, the path that packets follow have many opportunities to tamper with application data, sinkhole attacks can enable many other attacks (selective forwarding, for example). Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm.

Sybil attacks: In a Sybil attack , a single node presents multiple identities to other nodes in the network. The Sybil attack can significantly reduce the effectiveness of fault-tolerant schemes such as distributed storage, dispersity and multipath routing, and topology maintenance. Replicas, storage partitions, or routes believed to be using disjoint nodes could in actuality be using a single adversary presenting multiple identities. Sybil attacks also pose a significant threat to geographic routing protocols.

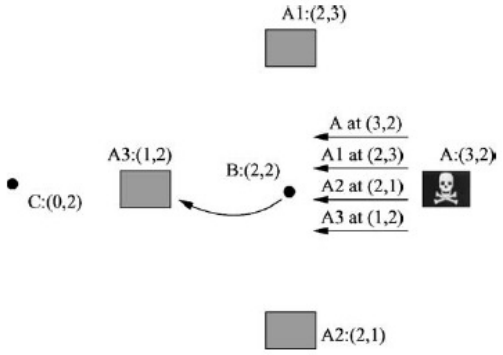

Fig.2: The Sybil attack against geographic routing. Adversary A at actual location (3,2) forges location advertisements for non-existent nodes A1, A2, and A3 as well as advertising her own location. After hearing these advertisements, if B wants to send a message to destination (0,2), it will attempt to do so through A3. This transmission can be overheard and handled by the adversary A.

Wormholes: In the wormhole attack, an adversary tunnels messages received in one part of the network over a low-latency link and replays them in a different part. The simplest instance of this attack is a single node situated between two other nodes forwarding messages between the two of them.

HELLO flood attacks: Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbors, and a node receiving such a packet may assume that it is within (normal) radio range of the sender. This assumption may be false: a laptop-class attacker broadcasting routing or other information with large enough transmission power could convince every node in the network that the adversary is its neighbor.

Acknowledgment spoofing: Several sensor network routing algorithms rely on implicit or explicit link layer acknowledgements. Due to the inherent broadcast medium, an adversary can spoof link layer acknowledgments for ‘‘overheard’’ packets addressed to neighboring nodes. Goals include convincing the sender that a weak link is strong or that a dead or disabled node is alive. For example, a routing protocol may select the next hop in a path using link reliability. Artificially reinforcing a weak or dead link is a subtle way of manipulating such a scheme. Since packets sent along weak or dead links are lost, an adversary can effectively mount a selective forwarding attack using acknowledgement spoofing by encouraging the target node to transmit packets on those links.

Protocol	**Relevant attacks**
TinyOS Beaconing	Bogus routing information, Selective forwarding, Sink holes, Sybil, Wormholes, HELLO floods
Directed diffusion and its multipath variant	Bogus routing information, Selective forwarding, Sink holes, Sybil, Wormholes, HELLO floods
Geographic routing (GPSR, GEAR)	Bogus routing information, Selective forwarding, Sybil
Minimum cost forwarding	Bogus routing information, Selective forwarding, Sink holes, Wormholes, HELLO floods
Clustering based protocols (LEACH , TEEN , PEGASIS)	Selective forwarding, HELLO floods
Rumor routing	Bogus routing information, Selective forwarding, Sink holes, Sybil, Wormholes
Energy conserving topology maintenance (SPAN , GAF, CEA, AFECA)	Bogus routing information, , Sybil, HELLO floods

Table 1: Relevant attacks found in the various kinds of proposed WSN protocols

3. KEY MANAGEMENT SCHEMES IN WSN

Many key management schemes for wireless sensor networks have been proposed in the past .In a wireless sensor network, the sensor nodes can be easily captured by an attacker. All of the information in the captured sensor nodes will thus be revealed and the attacker can obtain the encryption keys. We refer to this problem as the node capturing problem. For the key management schemes which are not based on the **r**andom **k**ey **p**re-distribution (RKP) scheme, the sensor nodes only store their own link keys. The **r**andom **k**ey **p**re-distribution (RKP) scheme is one which constructs a key pool which consists of a large number of keys. Each sensor node then randomly picks a certain number of keys from the key pool and stores them into its memory before it is deployed. The basic idea of this scheme is that any two sensor nodes have a probability of picking the same key from the key pool and this key can be used as their link key if these two sensor nodes want to establish a secure communication. When a sensor node is captured, only its own link keys will be revealed. In contrast, for the random key pre-distribution based schemes, the node capturing problem leads to the following problem. In , RKP based schemes, each sensor node stores its own link keys and some other possible link keys. When a sensor node is captured, the link keys that are not used by this sensor node may be revealed. In other words, when a sensor node is captured in a wireless sensor network using the RKP scheme, this captured node will reveal additional information about the link keys of the other sensor nodes. The node capturing problem is inevitable in a wireless sensor network. In order to alleviate the impact of node capturing problem for the RKP based schemes.

3.1 Key-Pre-distribution Protocols

In this section, we look into some key-pre-distribution protocols as proposed in the literature of [4], especially for WSNs. Because of their limitations on the computational power and their storage, it is often impossible to use any asymmetric-key infrastructure. Thus, key agreement and key pre-distribution are more important for WSNs than for traditional networks. In the literature, most of the study of key-pre-distribution protocols is based on random-graph theory. Although random-graph theory captures the randomness of wireless communications, it cannot capture the fact that the wireless communication range is limited: Two wireless nodes can communicate with each other only if they are within a certain distance. Thus, we mainly concentrate on the random-geometry-graph model. The random-geometry graph is more suitable for the sensor network because it treats the connectivity of each link by a probability and it also captures the fact that every node has a fixed geometry location.

Key pre-distribution for WSNs has drawn considerable research attention recently. Obviously, a number of naive methods could be used for the key-distribution problem. The simplest one may be the master key approach, in which every sensor node uses the same key in the whole network. This approach clearly is the most memory-efficient but has a low security because compromising one node will compromise the whole network. The other approach is to use a pair wise key. Each node stores $n - 1$ keys

in the sensor network of n nodes and uses a different key to communicate with different nodes. This approach achieves the highest security because compromising one link will not affect any other links. However, because n is typically large, each sensor node in the network should have large memory to store n − 1 keys. This is impractical because a sensor node has a very limited memory. Furthermore, it will be difficult to add a new node to the network after the key deployment because we need to add a new key at every existing sensor node for the secure communication to this new node. To achieve security in ad hoc networks, a number of protocols are based on public key encryptions (e.g., Hubaux et al., 2001; Kong et al., 2001). However, the public-key system is well beyond the capacities of current sensor nodes. It typically requires several minutes to generate keys with a Palm Pilot, and even a RSA signature takes tens of seconds. Several secure routing protocols based on symmetric-key encryption have been proposed for WSNs (e.g., Hu et al., 2001, 2002; Basagni et al., 2001). Perrig et al. (2001) present two security protocols optimized for use in sensor networks: SNEP and μTESLA. The SNEP protocol provides confidentiality, authentication, and freshness between nodes and the sink. The μTESLA protocol provides an authenticated broadcast. Both are useful building blocks for securing routing protocols in sensor networks.

The communication of a wireless sensor network can be eavesdropped quite easily due to its properties [11], thereby requiring a security mechanism. Adding a key management scheme on the wireless sensor network is a kind of solution as proposed by Tzu-Hsuan Shan and Chuan-Ming Liu. Using a little additional memory and computation, the proposed approach reduces the amount of information revealed when a sensor node is captured and thus makes a wireless sensor network that uses the random key pre-distribution scheme more secure. They analyzed the proposed approaches by considering two measurements: ACL (number of additional compromised links) and AID (the average insecurity degree). ACL measures the resilience against the node capturing problem and AID measures the security of each link key. Their experimental results match the analysis and show that the security of the wireless sensor network is enhanced about 50%.

4. STOCHASTIC ROUTING PROTOCOLS FOR SECURITY

There are a number of algorithms (e.g., Bohacek et al., 2002a, 2002b; Kodialam and Lakshman, 2003; Lee et al., 2005; Stone, 2000) proposed in their literature to achieve various security methods in wireless networks. The stochastic routing is designed to reduce the probability of successful prediction. Wireless networks pose some additional challenges and also additional opportunities for designing a saddle-routing policy. The challenge comes from the fact that wireless interference often makes an optimal routing problem NP-hard while the counterpart problem in the wired networks is polynomial-time solvable. A typical example of such problems is to find the largest throughput using a multipath routing between a pair of nodes; see Alicherry et al. (2005) and W. Wang et al. (2006b) for details. Y. Wu et al. (2007) consider a multihop, multichannel wireless networks and assume that the routing policy maker can jointly optimize the multipath routing and the link and channel scheduling. They assume that each node has only one radio because the majority of wireless nodes have only one NIC. For link scheduling, they consider synchronized TDMA because this will achieve more throughput than the

CSMA contention-based approach (Alicherry et al., 2005; Kumar et al., 2005;W.Wang et al., 2006b)

5. SPREAD: A multipath routing mechanism

We investigate the proposed SPREAD scheme the work of , Wenjing Lou,Wei Liu, Yanchao Zhang, Yuguang Fan, as a complementary mechanism to enhance secure data delivery in a mobile ad hoc network. The basic idea is to transform a secret message into multiple shares, and then deliver the shares via multiple paths to the destination so that even if a certain number of message shares are compromised, the secret message as a whole is not compromised. Three major design issues: the mathematical model for the generation and reconstruction of the secret message shares, the optimal allocation of the message shares onto multiple paths in terms of security, and the multipath discovery techniques in a mobile ad hoc network.

The fundamental idea of the SPREAD scheme comes from the following observation: a messenger who carries the full message from one place to another place across a hostile ground may reveal the message easily if he/she is captured, while the message will not be fully recovered by adversaries if multiple messengers are deployed, each only carrying partial information and taking different routes across the hostile ground. The SPREAD scheme works in the similar fashion: when a source node wants to send a message to a destination node securely in a MANET(Mobile Ad hoc network) , the source can use a multipath routing algorithm to find multiple paths from the source to the destination with certain properties (e.g., disjoint paths); then the source determines a secret sharing scheme, depending on the message security level and the availability of multiple paths, to transform the message into multiple shares; then the message shares are routed to the destination by the multipath routing protocol and the destination reconstructs the original message upon receiving a certain number of shares. There are several major design issues in this scheme: first, how to transform the message into multiple shares; secondly, how to allocate the shares onto each path; and thirdly, how to discover the desired multiple paths.

The first issue is how to divide the message into multiple pieces (shares)? The threshold secret sharing algorithm to divide the message into multiple pieces. With a (T, N) secret sharing algorithm, the secret message can be divided into N pieces (called message shares) such that in order to compromise the message, the adversary must compromise at least T shares. With fewer than T shares, the enemy cannot learn anything about the message and has no better chance to recover the secret than an outsider who knows nothing at all about the message. This gives us the desirable security properties. Another reason that we use secret sharing is that the generation of the message shares and the reconstruction of the message are all linear operations over a finite field. The second issue is how to allocate the shares onto each selected path so that the adversary has least possibility to compromise the message. The simplest and most intuitive share allocation scheme is to choose N as the number of available paths, apply (N, N) secret sharing, and allocate one share onto each path. This will achieve the desired maximum security with least processing cost. However, in an ad hoc network, wireless links are instable and the topology changes frequently. Packets might be dropped during the transmission. In case that packet loss does occur, this type of non-redundant share allocation will disable the reconstruction of the message even at the intended destination. The third issue is the multipath routing—how to find the desired multiple paths in a mobile ad hoc network and

how to deliver the shares to the destination using these paths? Routing in a MANET presents great challenge because the nodes are capable of moving and the network topology can change continuously, dramatically, and unpredictably. SPREAD scheme, we need independent paths, more specifically, node-disjoint paths, as many as possible, because we are dealing with node compromise problem

6. CONCLUSION

Security is sometimes viewed as a standalone component of a system's architecture and especially in case of wireless sensor network, where a separate module provides security. This separation is, however usually a flawed approach to network security. To achieve a secure system, security must be integrated into every component, since components designed without security can become a point of attack. Consequently, security must pervade every aspect of the system design in WSN. In the future, we may expect to see research on a even better random-key pre distribution schemes providing resilience to node compromise, as well as investigation of hardware support for public-key cryptography and more efficient public-key schemes (such as elliptic curve cryptography). Though cryptography entails a performance cost for extra computation that often increases packet size, it should be optimally considered as cryptographic hardware support too increases efficiency increasing the financial cost of implementing a network. . Many applications are likely to involve the deployment of sensor networks under a single administrative domain, simplifying the threat model.Hence, an important question facing sensor node researchers and practitioners is: Can reasonable security and performance levels be achieved with software- only cryptographic implementations, or is hardware support needed or is there a need for a different way of sensor deployment? Recent research demonstrates that software-only cryptography is indeed practical with today's sensor technology; hardware support is not needed to technology alone is unlikely to be able to solve the privacy problem; rather, a mix of societal norms, new laws, and technological responses are necessary. Providing awareness of the presence of sensor nodes and data acquisition is particularly important. Affected parties aware of the existence form and implications of surveillance are more likely to accept the technology. However, our current understanding of privacy in sensor networks itself is immature, rest alone is the security measures of sensors that communicate in the wireless standards and this obviously demands more research.

7. REFERENCES

[1] Wenjing Lou,Wei Liu, Yanchao Zhang, Yuguang Fanm,"SPREAD:Improving network security by multipath routing in mobile ad hoc networks",Springer Wireless Networks (2009) 15:279–294)

[2] F.Akyildiz, W.Su, Y.Sankarasubramaniam, and E.Cayirci," Wireless sensor networks: a survey", Computer Networks 38:393–422, 2002.

[3] A.Cerpa, J.Elson, D. Estrin, L. Girad, M. Hamilton, and J. Zhao," Habitat monitoring: Application driver for wireless communication technology, In Proceedings of ACM SIGCOMM Workshop on Data Communications in Latin America and the Caribbean, pages 3–5, 2001.

[4] D.J. Malan, M. Welsh, and M.D. Smith ,"A Public-Key Infrastructure for Key Distribution in Tinyos Based on Elliptic Curve Cryptography", In Proceedings of the First IEEE Intl Conf. Sensor and Ad Hoc Comm. and Networks, 2004.
[5] A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, and D.E. Culler," SPINS: Security Protocols for Sensor Networks", In Wireless Networks, vol. 8, pages. 521 - 534, 2003.
[6] M. Ramkumar and N. Memon ,"An Efficient Random Key Predistribution Scheme, In Proceedings of the IEEE Global Telecomm Conference, 2004.
[7] H. Chan and A. Perrig, W. Lou and Y. Fang ," A survey on wireless security in mobile ad hoc networks: Challenges and available solutions",book chapter in: Ad Hoc Wireless Networking (Kluwer, May 2003).
[8] J. Kong, P. Zerfos, H. Luo, S. Lu and L. Zhang,"Providing robust and ubiquitous security support for manet", in ,ICNP (2001)
[9] L. Eschenauer and V. Gligor W. Du, J. Deng,Y. Han and P.Varshney," A pair wise key pre distribution scheme for wireless sensor networks", in: ACMCCS 03 (2003).
[10] H. Chan, A. Perrig and D. Song," Random key predistribution schemes for sensor networks", in: IEEE Symposium on Security and Privacy (SP'03) (Oakland, CA, May 2003).
[11] S. Zhu, S. Xu, S. Setia and S. Jajodia, "Establishing pairwise keys for secure communication in ad hoc networks: A probabilistic approach".in: 11th IEEE Internationaal Conference on Network Protocols (ICNP'03) (Atlanta, GA, November 2003)