Research Article Impact Factor: 0.621 ISSN: 2319-507X
Sheetal Yawalkar, IJPRET, 2014; Volume 2 (9): 785-792 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

AN OVERVIEW OF COMMUNICATION PROTOCOLS IN WIRELESS SENSOR NETWORK

SHEETAL M. YAWALKAR.

Bhartiya Mahavidhyalaya, Amravati, Ms, India.

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: Popularity of wireless sensor networks (WSNs) is increasing continuously in different domains of daily life, as they provide efficient method of collecting valuable data from the surroundings for use in different applications. Due to distributed nature of these networks and their deployment in remote areas, these networks are vulnerable to numerous security threats that can adversely affect their proper functioning. This problem is more critical if the network is deployed for some mission-critical applications such as in a tactical battlefield. Random failure of nodes is also very likely in real-life deployment scenarios. Due to resource constraints in the sensor nodes, traditional security mechanisms with large overhead of computation and communication are infeasible in WSNs. Security in sensor networks is, therefore, a particularly challenging task. This paper discusses the current state of the art in security mechanisms for WSNs. Various types of attacks are discussed and their countermeasures presented. A brief discussion on the future direction of research in WSN security is also included.

Keywords: Wireless Sensor Network security, SNEP , µTESLA.

Corresponding Author: MS. SHEETAL M. YAWALKAR

Access Online On:

www.ijpret.com

How to Cite This Article:

Sheetal Yawalkar, IJPRET, 2014; Volume 2 (9): 785-792

PAPER-QR CODE

INTRODUCTION

In future, there will be thousands to millions of small sensors forming self-organizing wireless networks. These sensor networks are characterized by limited power and energy supplies, low bandwidth, small memory size, unreliable communication (e.g.unreliable transfer, conflicts and latency) and unattended operation. Therefore traditional security techniques in computer networks are not suitable and useful for wireless sensor networks. Some applications are listed below

- *Energy management*

In 2001 power blackouts plagued California. Energy distribution will be better managed when we begin to use remote sensors. For example,

The power load that can be carried on an electrical line depends on ambient temperature and the immediate temperature on the wire. If these were monitored by remote sensors and the remote sensors received information about desired load and current load, it would be possible to distribute load better. This would avoid circumstances where Californians cannot receive electricity while surplus electricity exists in other parts of the country.

- *Medical monitoring*

We envision a future where individuals with some types of medical conditions receive constant monitoring through sensors that monitor health conditions. For some types of medical conditions, remote sensors may apply remedies (such as instant release of emergency medication to the bloodstream).

- *Logistics and inventory management*

Commerce in America is based on moving goods, including commodities from locations where surpluses exist to locations where needs exist. Using remote sensors can substantially improve these mechanisms. These mechanisms will vary in scale . ranging from worldwide distribution of goods through transportation and pipeline networks to inventory management within a single retail store.

- *Battlefield management*

• Remote sensors can help eliminate some of the confusion associated with combat. They can allow accurate collection of information about current battlefield conditions as well as giving appropriate information to soldiers, weapons, and vehicles in the battlefield.

II. SECURITY OF SENSORS

These constraints make it impractical to use the majority of the current secure algorithms, which were designed for powerful workstations. For example, the working memory of a sensor node is insufficient to even hold the variables (of sufficient length to ensure security) that are required in asymmetric cryptographic algorithms (e.g. RSA[1], Diffie-Hellman[2]). Let alone perform operations with them. A particular challenge is broadcasting authenticated data to the entire sensor network. Current proposals for authenticated broadcast are impractical for sensor networks. Most proposals rely on asymmetric digital signatures for the authentication, which are impractical for multiple reasons (e.g. long signatures with high communication overhead of 50-1000 bytes per packet, very high overhead to create and verify the signature).TESLA is efficient for the Internet with regular desktop workstations, but does not scale down to our resource-starved sensor nodes. In this paper, we extend and adapt TESLA such that it becomes practical for broadcast authentication for sensor networks. We call this new protocol µTESLA .The measurements show that adding security a highly resource-constrained sensor network is feasible. The paper studies an authenticated routing protocol and a two-party key agreement protocol, and demonstrates that our security building blocks greatly facilitate the implementation of a complete security solution for a sensor network.

III. KEY FEATURES FOR SENSOR NETWORK SECURITY

In this section, we formalize the security properties required by sensor networks, and show how they are directly applicable in a typical sensor network.

A. Data Confidentiality: A sensor network should not leak sensor readings to neighboring networks. In many applications (e.g. key distribution) nodes communicate highly sensitive data.

B. Data Authentication:

Message authentication is important for many applications in sensor networks. Within the building sensor network, authentication is necessary for many administrative tasks (e.g. network reprogramming or controlling sensor node duty cycle). At the same time, an Adversary can easily inject messages, so the receiver needs to make sure that the data used in any decision-making process originates from the correct source. Informally, data authentication allows a receiver to verify that the data really was sent by the claimed sender.

C. Data Integrity

In communication, data integrity ensures the receiver that the received data is not altered in transit by an adversary. In SPINS, we achieve data integrity through data authentication, which is a stronger property. Data Freshness Given that all sensor networks stream some forms of

time varying measurements, it is not enough to guarantee confidentiality and authentication; we also must ensure each message is fresh.

IV. SPINS SECURITY BUILDING BLOCKS

To achieve the security requirements we established in Section 3 we have designed and implemented two security building blocks: SNEP and µTESLA. SNEP provides data confidentiality, two-party data authentication, integrity, and freshness. µTESLA provides authentication for data broadcast. We bootstrap the security for both mechanisms with a shared secret key between each node ad the base station.

A. SNEP

SNEP provides a number of unique advantages. First, it has low communication overhead since it only adds 8 bytes per message. Second, like many cryptographic protocols it uses a counter, but we avoid transmitting the counter value by keeping state at both end points. Third, SNEP achieves even semantic security, a strong security property which prevents eavesdroppers from inferring the message content from the encrypted message. Finally, the same simple and efficient protocol also gives us data authentication, replay protection, and weak message freshness. Data confidentiality is one of the most basic security primitives and it is used in almost every security protocol.. The basic technique to achieve this is randomization: Before encrypting the message with a chaining encryption function (i.e. DES-CBC), the sender precedes the message with a random bit string. This prevents the attacker from inferring the plaintext of encrypted messages if it knows plaintext-cipher text pairs encrypted with the same key. However, sending the randomized data over the RF channel requires more energy. So we construct another cryptographic mechanism that achieves semantic security with no additional transmission overhead. Instead, we rely on a shared counter between the sender and the receiver for the block cipher in counter mode (CTR). Since the communicating parties share the counter and increment it after each block, the counter does not need to be sent with the message. To achieve two-party authentication and data integrity, we use a message authentication code.(MAC).The combination of these mechanisms forms our Sensor Network Encryption Protocol SNEP.

SNEP offers the following nice properties:

- *Semantic security*

Since the counter value is incremented after each message, the same message is encrypted differently each time. The counter value is long enough that it never repeats within the lifetime of the node.

- *Data authentication*

If the MAC verifies correctly, a receiver can be assured that the message originated from the claimed sender.

- *Replay protection*

The counter value in the MAC prevents replaying old messages. Note that if the counter were not present in the MAC, an adversary could easily replay messages.

- *Weak freshness*

If the message verified correctly, a receiver knows that the message must have been sent after the previous message it received correctly (that had a lower counter value). This enforces a message ordering and yields weak freshness.

- *Low communication overhead*

The counter state is kept at each end point and does not need to be sent in each message.

B. µTESLA

Current proposals for authenticated broadcast are impractical for sensor networks. First, most proposals rely on asymmetric digital signatures for the authentication, which are impractical for multiple reasons. They require long signatures with high communication overhead of 50-1000 bytes per packet, very high overhead to create and verify the signature. Even previously proposed one-time signature schemes that are based on symmetric cryptography (one-way functions without trapdoors) have a high overhead: Gennaro and Rohatgi's broadcast signature based on Lamport's one-time signature[3] requires over 1 Kbyte of authentication information per packet[4] , and Rohatgi's improved k-time signature scheme requires over 300 bytes per packet[5]. The recently proposed TESLA protocol provides efficient authenticated broadcast [6][7]. However, TESLA is not designed for such limited computing environments as we encounter in sensor networks for three reasons. too expensive to compute on our sensor nodes, since even fitting the code into the memory is a major challenge. For the same reason as we mention above, onetime signatures are a challenge to use on our nodes. Standard TESLA has an overhead of approximately 24 bytes per packet. For networks connecting workstations this is usually not significant. Sensor nodes, however, send very small messages that are around 30 bytes long. It is simply impractical to disclose the TESLA key for the previous intervals with every packet: with 64 In case the MAC does not match, the receiver can try out a fixed, small number of counter increments to recover from message loss. In case the optimistic re-synchronization fails, the two parties engage in a counter exchange protocol, which uses the

strong freshness protocol described below. bit keys and MACs, the TESLA-related part of the packet would be constitute over 50% of the packet. Finally, the one-way key chain does not fit into the memory of our sensor node. So pure TESLA is not practical for a node to broadcast authenticated data.

V. APPLICATIONS

In this section we demonstrate how we can build secure protocols out of the SPINS secure building blocks. First, we build an authenticated routing application, and second, a two-party key agreement protocol. Using the µTESLA protocol, we developed a lightweight, authenticated ad hoc routing protocol that builds an authenticated routing topology. Ad hoc routing has been an active area of research[15] .However, none of these solutions offer authenticated routing messages. Hence it is potentially easy for a malicious user to take over the network by injecting erroneous, replaying old, or advertise incorrect routing information. The authenticated routing scheme we developed mitigates these problems. The routing scheme within our prototype network assumes bidirectional communication channels, i.e. if node A hears node B, then node B hears node A.

The route discovery depends on periodic broadcast of beacons. Every node, upon reception of a beacon packet, checks whether it has already received a beacon (which is a normal packet with a globally unique sender ID and current time at base station, protected by a MAC to ensure integrity and that the data is authentic) in the current epoch 5. If a node hears the beacon within the epoch, it does not take any further action. Otherwise, the node accepts the sender of the beacon as its parent to route towards the base station. Additionally, the node would repeat the beacon with the sender ID changed to itself. This route discovery resembles a distributed, breadth first search algorithm. However, in the above algorithm, the route discovery depends only on the receipt of route packet, not on its contents. It is easy for any node to claim to be a valid base station. We note that the µTESLA key disclosure packets can easily function as routing beacon. We accept only the sources of authenticated beacons as valid parents. Reception of a µTESLA packet guarantees that that packet originated at the base station, and that it is fresh. For each time interval, we accept as the parent the first node that sends a packet that is later successfully authenticated. Combining µTESLA key disclosure with the distribution of routing beacons allows us to charge the costs of the transmission of the keys to network maintenance, rather than the encryption system. This scheme leads to a lightweight authenticated routing protocol. Since each node accepts only the first authenticated packet as the one to use in routing, it is impossible for an attacker to reroute arbitrary links within the sensor network. Furthermore, each node can easily verify whether the parent forwarded the message: by our assumption of bidirectional connectivity.

VI. CONCLUSION

We have successfully demonstrated the feasibility of security subsystem for an extremely limited sensor network platform. We have identified useful security protocols for sensor networks: authenticated and confidential communication, and authenticated broadcast. Many elements of design are universal and apply easily to other sensor networks. Since our primitives are solely based on fast symmetric cryptography, and use no asymmetric algorithms, our building blocks are applicable to a wide variety of device configurations. The computation costs of symmetric cryptography are low. Since the data authentication, freshness, and confidentiality properties require transmitting a mere 8 bytes per unit, it is feasible to guarantee these properties on a per packet basis, even with small 30 byte packets. It is difficult to improve on this scheme, as transmitting a MAC is fundamental to guaranteeing data authentication. A more powerful device would also allow for more basic modes of authentication.

REFERENCES

1. D. Johnson and D.A. Maltz and J. Broch. The dynamic source routing protocol for mobile ad hoc networks (internet-draft). In Mobile Ad-hoc Network (MANET) Working Group, IETF, October 1999.

2. Joan Daemen and Vincent Rijmen. AES propos Rijndael,March1999

3. W. Diffie and M. E. Hellman. New directions in cryptography. IEEE Trans. Inform. Theory, IT-22:644–654, November 1976.

4. Whitfield Diffie and Martin E. Hellman. Privacy and authentication: An introduction to cryptography. Proceedings of the IEEE, 67(3):397–427, March 1979.

5. Armando Fox and Steven D. Gribble. Security on the move: indirect authentication using Kerberos. In Second Annual International Conference on Mobile Computing and Networking (MOBICOM 1996), pages 155–164, White Plains, NY USA, November 1996.

6. R. Gennaro and P. Rohatgi. How to sign digital streams. In Burt Kaliski, editor, Advances in Cryptology - Crypto '97, pages 180–197, Berlin, 1997. Springer-Verlag. Lecture Notes in Computer Science Volume 1294.

7. Shafi Goldwasser and Silvio Micali. Probabilistic encryption.Journal of Computer Security, 28:270–299, 1984.

8. Z.J. Haas and M. Perlman. The zone routing protocol (ZRP)for adhoc networks (Internet-Draft). 1998.

9. Neil M. Haller. The S/KEY one-time password system. In ISOC, 1994.

10. D. Harkins and D. Carrel. The internet key exchange (IKE).Request for Comments 2409, Information Sciences Institute, University of Southern California, November 1998.

11. J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister. System architecture directions for networked sensors. In Proceedings of the 9th International Conference on Architectural Support for Programming Languages and Operating Systems, November 2000.

12. D.B. Johnson and D.A. Maltz. Dynamic source routing in ad-hoc wireless networks. In Mobile Computing, 1996.

13. Young-Bae Ko and Nitin Vaidya. Location-aided routing (LAR) in mobile ad hoc networks. In Proceedings of the Fourth International Conference on Mobile Computing and Networking (MobiCom'98), October 1998.

14. L. Lamport. Constructing digital signatures from a one-way function. Technical Report CSL-98, SRI International, October 1979.

15. H. Lipmaa, P. Rogaway, and D. Wagner. Counter mode encryption.

16. http://csrc.nist.gov/encryption/modes/.

17. Alfred J. Menezes, Paul van Oorschot, and Scott Vanstone. Handbook of Applied Cryptography. CRC Press, 1997.

18. S. P. Miller, C. Neuman, J. I. Schiller, and J. H. Saltzer. Kerberos authentication and authorization system. In Project Athena Technical Plan, page section E.2.1, 1987.

19. N. Modadugu, D. Boneh, and M. Kim. Generating RSA keys on a handheld using an untrusted server. In RSA 2000, 2000.

20. NIST. Advanced encryption standard (AES) development Effort http://csrc.nist.gov/encryption/aes/, October 2000.

21. V.D. Park and M.S. Corson. A highly adaptable distributed routing algorithm for mobile wireless networks. In IEEE INFOCOMM'97, 1997.

22. Bhrat Patel and Jon Crowcroft. Ticket based service access for the mobile user. In Third annual ACM/IEEE international conference on Mobile computing and networking, pages 223–233, Budapest Hungary, September 1997.

23. C.E. Perkins and P. Bhagwat. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In ACM SIGCOMM Symposium on Communication, Architectures and Applications, 1994.