Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.1197 – 1203

RESEARCH ARTICLE

A Secure Routing Protocol under Eavesdropping using SPENA Scheme

Mohini Singhal[1], Kaushik Ghosh[2]

[1]M.tech (CSE), Mody University of Science & Technology, Laxmangarh (Sikar), India

smohini2111@gmail.com

[2]Assistant Professor, Department of Computer Science and Engineering, Mody University of Science & Technology, Laxmangarh (Sikar), India

Abstract— In a wireless sensor network, an important problem is to provide privacy to the detecting sensor node and integrity to the data gathered by a node. In addition to the reliability, communication security is another important concern in wireless networks, since the wireless transmission is highly vulnerable to eavesdropping attacks due to the open nature of wireless medium. In eavesdropping we introduce transmission scheme; all relay and best relay and analysed the intercept behavior in wireless networks. Here we introduce a secure protocol TinyPK and TinySec which prevent from eavesdropping attack. Here we present a scheme to hide source information. The packet is modified en route by dynamically selected nodes to make it difficult for a malicious entity to trace back the packet to a source node and also prevent packet spoofing. Evaluating the proposed work through both simulation and analysis, we show proposed protocol can significantly outperform the closest routing protocol and security mechanism.

Keywords— Include Eavesdropping, TinyPK, TinySec

I. INTRODUCTION

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to cooperatively monitor physical or environment condition, such as temperature, sound, vibration, pressure, motion or pollutants. The development of wireless sensor networks was motivated by

Military application such as battlefield surveillance[1]. A WSN consist of hundred or even thousands of small devices each with sensing, processing, and communication capabilities to monitor a real-world environment. The sensor nodes use wireless transmission, which is out in the open and can be overheard in the communication vicinity. Without precaution, a malicious entity overhearing packet transmission can trace back the packet to the source[13]. This can be lead to the position of the source along with the location and time of event occurrence. The popularity of sensor network application is aided by the form factor and the cost of the sensor node. The sensor node use wireless transmission, which is out in the open and can be overheard in the communication. Without precaution, a malicious entity overhearing packet transmission can trace back the Packet to the source[2].

This paper aims to maintain source privacy under eavesdropping and node compromise attacks. We use one way hash chain based keying mechanism to hide the source information. This is further used to obfuscate an additional partial hash by dynamically selected nodes preventing a trace back by the adversary.

II. PROBLEM STATEMENT

The Threat model allows the adversary to super-locally eavesdrop, while also being able to compromise nodes. In Super-local eavesdropping, the adversary eavesdrops over a local area but can overhear communication over significantly larger coverage area than a sensor node[3]. An example of an adversary is a laptop class attacker. When a node is compromised, an adversary has access to all the cryptographic information available to the node.

III. PROPOSED TECHNIQUE

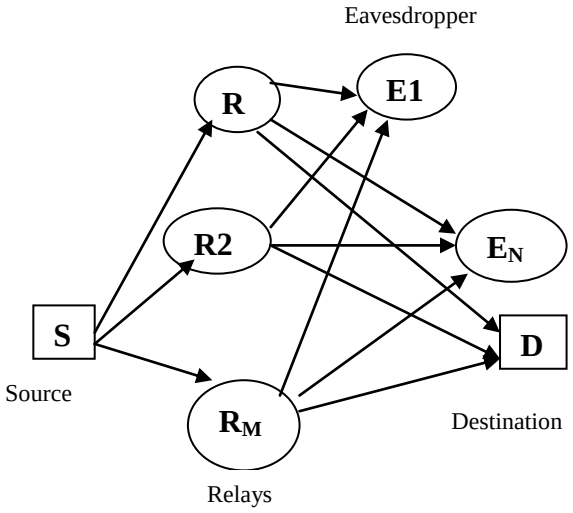

Figure 1 A collaborative wireless network consisting of a source, a destination and *M* relays in the presence of *N* eavesdroppers[4].

There has been a lot of work to consolidate the security principles in wireless sensor network.

To defend against eavesdropping attacks and a noise-forwarding scheme was proposed by allowing a relay node to send artificial noise to confuse eavesdroppers[4].

In [5], Jung, et al. presented the transmission power control for security improvement in ad-hoc wireless network has been addressed and analyzed the impact of the transmission range and user distribution on the eavesdropping risk, when there is one or more adversarial nodes.

In [6], Roosta, et al. presented a taxonomy attacks on sensor network and emphasized how analysis attack traffic can leak source information.

In [7], Waldir, et al. provide protocols for detecting suspicious transmission and the consequent identification of malicious node and for disseminating this information in the network.

IV. ROUTING PROTOCOL

Here we introducing two protocol: TinyPK and TinySec, are secure under eavesdropping.

4.1. TINYPK: SENSOR NETWORKS WITH PUBLIC KEY TECHNOLOGY

Here we describe about public-key-(PK)-based protocols that allow authentication and key agreement between a sensor network and a third party as well as between two sensor networks. In many sensor network applications, security and privacy of the data collected will be a critical concern. Providing security services for sensor networks is a technical challenge. The low power design objective for the sensor nodes forces security mechanisms to fit under very limiting processing and bandwidth constraints.[8] Our expectation is that secure symmetric encryption will be widely available on the sensor networks of the future. The critical problem is making effective use of that secure symmetric encryption capability. As is always the case with symmetric encryption, proper key management is a fundamental concern. Public key (PK) technology is a widely used tool to support symmetric key management in the realm of Internet hosts and high-bandwidth interconnections. There are several security problems that are beyond the scope of our current work. For example, we do not handle the problem of revocation of compromised private keys. We also have designed only limited protection against denial of service attacks.

The TinyPK implementation uses the RSA algorithm to exploit its speed in public key operations. Currently, our implementation of RSA private operations is too slow to be used on motes, as extrapolations indicated that execution times would be in the tens of minutes[12].

After some validation tests which demonstrated a noticeable speed improvement, we implemented Diffie-Hellman key exchange. The goal of Diffie-Hellman is to provide a shared secret between two parties that can then be use to create a cryptographic key. We use Diffie-Hellman to generate a secret suitable for use in creating a new or replacement TinySec key. Such a key would allow two disjoint sensor networks to communicate and allow the deployment of replacement motes into an existing sensor field without having to look up and preload the TinySec key in use by the field. The protocol operates in the standard manner: The mote initiates the exchange by generating a random number R1, performing the blinding function (i.e. calculating g R1 mod p) and sending that quantity to another mote. The second mote generates its own random number, R2, and performs the blinding function in parallel with the first mote. Upon receipt of the blinded quantity, it responds by sending its blinded quantity to the first mote. Each mote then calculates

(g R1 mod p)R2 mod p = (g R2 mod p)R1 mod p = g R!*R2 mod p ,

which is the shared secret. In our current implementation of modular arithmetic, we use a generator, g=2, and have the capability of using exponents and module of differing sizes.[8] The nature of Diffie-Hellman is such

that the communications between parties can take place in an unsecured manner. This mode of operation is needed between two The TinyPK system demonstrates that a public-key based protocol is feasible for an extremely lightweight sensor network.

The Diffie-Hellman key exchange is susceptible to two attacks: the discrete logarithm attack and the Man-in-the-Middle attack.[9]

4.2. **TinySec: A Link Layer Security Architecture for Wireless Sensor Networks**

We introduce TinySec, the first fully-implemented link layer security architecture for wireless sensor network. We take this challenge and introduce TinySec[10], a lightweight, generic security package that developers can easily integrate into sensor network application. The design of TinySec based on existing security primitives that other researcher has proven to be secure. Here we describe a complete solution, defining packet formats and application interface, and provide a detailed performance characterization.

We explore some of the tradeoffs between performance, transparency, and cryptography security, and we explaining a design that meets needs of application in the sensor network space.

4.2.1. **Security primitives**

A common solution for achieving message integrity and authenticity is to use a message authentication code (MAC)[11]. A MAC requires authorized senders and receivers to share a secret key and this key is part of the input to a MAC computation. The sender computes a MAC over the packet with the secret key and includes the MAC with the packet. A receiver sharing the same secret key recomputed the MAC and compares it with the received MAC value. If they are equal, the receiver accepts the packet and rejects it otherwise.

Note that there is no need to use two channels in this case. Both message and the MAC can be sent on the same insecure channel. An intruder can see the message, but it cannot forge a new message to replace it because an intruder does not possess the secret key between source and destination. That is unable to create the same MAC as source did.

The MAC we have described is referred to as a prefix MAC because the secret key is appended to the beginning of the message. We can have a postfix MAC, in which the key is appended to the end of the message. We can combine the prefix MAC, with the same key or two different keys. However, the resulting MACs are still insecure.

V. SPENA SCHEME

SPENA is a source privacy protection scheme which uses one-way hash chains and mapping function.

In SPENA, a one way hash chain is used to hide the source information. A one-way hash chain is a series of hash values generated by a one-way hash function.[12] A basic idea of this approach is : First, a unique hash function is used to generate a hash for source identification. This function is available at the source node and the base station. Second, dynamically selected intermediate nodes on the routing path alter the packet resulting in a change to the packet structure.

DESTID	SRCID	OBFUSCATING PARTIAL HASH	REHASH SEED	PAYLOAD|SCRID	FILLER

Fig 2 Event Packet

SPENA can be used with a single path routing or a flooding based routing method. The event packet structure in SPENA is presented in figure 2, and it has following parameter:

1) DstID (Destination-id): It is the destination id of the packet. This is base station for event packets.
2) SrcID hash (Source-id Hash): A unique hash of the source that is used to identify it at the base station.
3) Obfuscating partial hash (OPH): This is generated by the source using the same hash function used to create the SrcID hash, and will be modified by dynamically selected intermediate nodes.
4) Rehash seed: Used to determine the intermediate nodes to reconstruct the packet en route to the base station.
5) Payload Length: The length of a payload in the packet.
6) Payload: Payload is the actual data transmitted in the packet. It is encrypted using the symmetric key shared by the source node and the base station.
7) Filler: Filler is used to provide a standard length to the packet and is populated with random garbage data.

Constant packet size is required to prevent the adversary from tracking the packet based on increase in packet length during packet transformation. Keeping all the packets with same length forces the adversary to consider all packets while tracking back and it cannot discount any packet analysis requirement based on the packet length.

VI. PACKET TRANSFORMATION SCENARIO

On receiving a valid packet presented in figure 3, the base station uses a sliding window approach to look for the source id corresponding to the SrcID hash within the sliding windows of the hash table maintained for each node. A sliding window approach helps to improve the efficiency since the base station does not need to go through the whole hash table. When the valid packet is received, the starting point of the window is moved beyond SrcID hash in the table corresponding to the source.

The base station, on receiving the packet does a reverse lookup on the SrcID hash to identify the source of the packet. It applies a recursive process as show in figure 3, until it reaches the true source id of the packet.

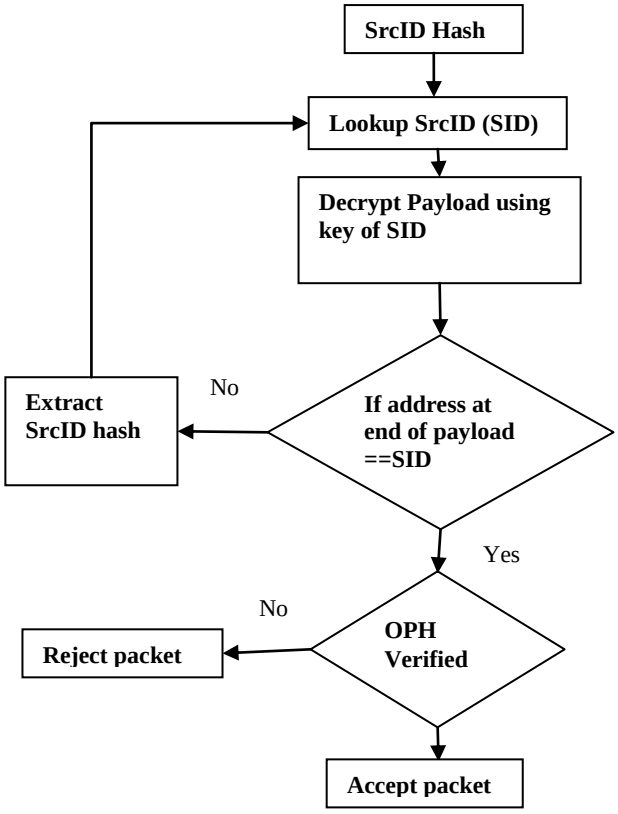

Fig 3 Packet Reception and Verification

During this process the base station identifies the intermediate nodes responsible for rehashing the obfuscating partial hash. If the base station reaches the same value as received in the packet, then this verifies the integrity of the packet received.

VII. CONCLUSION

In Wireless sensor network introducing sensor network with limitation and characteristic sensor nodes Here we use existing techniques consider an eavesdropping adversary and refrain from providing source privacy solutions to an intrusive node compromise attack under eavesdropping. The goal of the adversary is to identify the location and time of event occurrence, either by passive super-local eavesdropping or using intrusive node compromise.

In this work, we first present two protocols: TinySec and TinyPK to provide security and to maintain integrity of data. We provide a packet verification method for the base station to validate a received packet. Finally this process is used to keep maintain integrity and authenticity of data.

REFERENCES

1. Pathan, Al-Sakib Khan, Hyung-Woo Lee, and Choong Seon Hong. "Security in wireless sensor networks: issues and challenges." Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference. ©IEEE, 2006.
2. Karlof, Chris, and David Wagner. "Secure routing in wireless sensor networks: Attacks and countermeasures." Ad hoc networks 1.2 (2003)

3. Zou, Yulong, Xianbin Wang, and Weiming Shen. "Eavesdropping attack in collaborative wireless networks: Security protocols and intercept behavior."Computer Supported Cooperative Work in Design (CSCWD), 2013 IEEE 17th International Conference on. IEEE, 2013.
4. Lai, Lifeng, and Hesham El Gamal. "The relay–eavesdropper channel: Cooperation for secrecy." Information Theory, IEEE Transactions on 54.9 (2008): 4005-4019
5. Kao, Jung-Chun, and Radu Marculescu. "Eavesdropping minimization via transmission power control in Ad-Hoc wireless networks." Sensor and Ad Hoc Communications and Networks, 2006. SECON'06. 2006 3rd Annual IEEE Communications Society on. Vol. 2. IEEE, 2006.
6. Roosta, Tanya, Shiuhpyng Shieh, and Shankar Sastry. "Taxonomy of security attacks in sensor networks and countermeasures." The First IEEE International Conference on System Integration and Reliability Improvements. Vol. 25. 2006.
7. Pires Jr, Waldir Ribeiro, et al. "Malicious node detection in wireless sensor networks."in "Parallel and Distributed Processing Symposium, 2004. Proceedings. 18th International". ©IEEE, doi: 10.1109/IPDPS.2004.1302934
8. Watro, Ronald, et al. "TinyPK: securing sensor networks with public key technology." Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks. ACM, 2004
9. Bresson, Emmanuel, Olivier Chevassut, and David Pointcheval. "Dynamic group Diffie-Hellman key exchange under standard assumptions." Advances in Cryptology—EUROCRYPT 2002. Springer Berlin Heidelberg, 2002.
10. Karlof, Chris, Naveen Sastry, and David Wagner. "TinySec: a link layer security architecture for wireless sensor networks." Proceedings of the 2nd international conference on Embedded networked sensor systems. ACM, 2004.
11. Gliwa, Rafał, and Wojciech Oszywa. "Message Authentication for Authenticated Encryption Scheme."
12. Pongaliur, Kanthakumar, and Li Xiao. "Maintaining source privacy under eavesdropping and node compromise attacks." In "INFOCOM" *2011,* © IEEE, doi: 10.1109/INFCOM.2011.5934959
13. Choi, Yong-Sik, Young-Jun Jeon, and Sang-Hyun Park. "A study on sensor nodes attestation protocol in a Wireless Sensor Network." In "Advanced Communication Technology (ICACT), 2010 The 12th International Conference on". ©IEEE, 2010.

