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
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 4, April 2016, pg.79 – 86

A NOVEL APPROACH TO DETECT INTRUSION USING DIFFIE HELLMAN AND BLOW FISH

Sumaiya Rashid, Sumit Wadhwa
rashidsumaiya10@gmail.com, sgisumitcse@gmail.com
Samalkha group of Institutions Samalkha, NH-1, Delhi NCR, 132115(HR.)

ABSTRACT: In the last decade the researchers did so many works in the field of security in wireless sensor network. They introduce different techniques of security but now they emphasize on the security of the location of source because if the attacker don't know the location of the source where the packet is to be generated, so the attacker have to monitor the whole network all the time to access the information. In order to protect the source location privacy, we propose a novel scheme based on the fake packet injection and routing real packets with fake packets. Every real packet is still routed along the shortest path, while the fake packets are routed to the sink with some fake sources. As a result, the path diversity is provided. An attacker cannot distinguish the real packets from the fake packets, so it is more difficult for an attacker to deduce the real source by packet tracing.

Keywords: Intrusion detection, Blow Fish, WSN, Fake packets, tracing.

I. INTRODUCTION

Wireless sensor networks (WSNs) are composed of a large number of sensor nodes that are self-organized to carry tasks in military and civilian applications such as battlefield surveillance, forest fire detection, patient health monitoring, and smart environment [1]. In a WSN, sensor nodes are densely deployed, so that neighbor nodes may be very close to each other. Hence, multi-hop communication in a WSN is most commonly used than a single-hop communication in order to consume less energy. Each node collects data from its environment and transports data to the receiver via a multi-hop network, performing the routing function. The open nature of WSNs makes it normally operate in unattended or hostile

environments, which is easily exposed to a variety of attacks such as eavesdropping, node compromising, and physical disruption.

Privacy in WSNs may be classified into data privacy and context privacy in Fig. 1 [2]. Even after strong encryption and authentication mechanisms are applied to protect data privacy, the context information such as the location information of the source or the receiver can be deduced by eavesdropping the network traffic and analyzing the traffic patterns. Context-oriented privacy protections can be split into location privacy preserving techniques and temporal privacy preserving techniques. Location privacy includes data source location protections and receiver location protections. Location privacy is extremely important in WSNs. In our work, we focus on the protection of the source location privacy in WSNs by using the novel approach that uses fake node and routing based source location privacy.

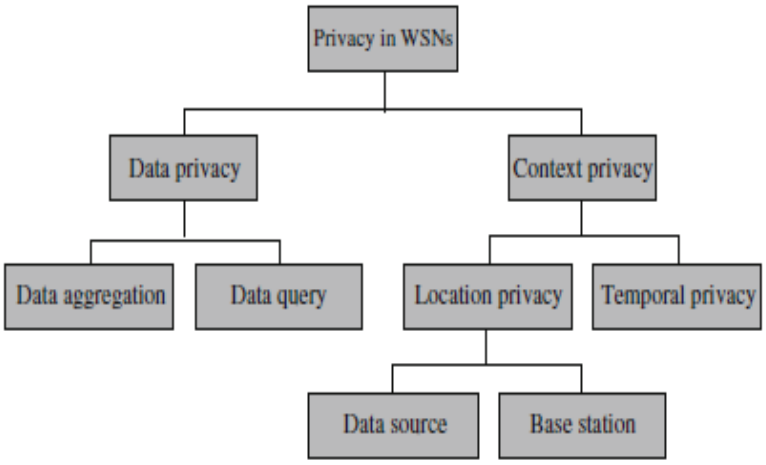

Figure 1: Taxonomy of privacy protection

A. WSN Architecture

There are various architectures for a WSN. Let us discuss a few of the different architectural aspects of a WSN. Note that this is only a short introduction to architectural aspects. For more details: see the literature list at the end of the thesis.

One sink - multiple sinks: A WSN can be organized in a topology with multiple sinks or a single sink. Nodes can send their data to the specific sink based on the topology or based on the type of data that a node has to send.

Data Centric WSN: A data-centric wireless sensor network is a special case of a WSN. In this WSN there is no sink available. Instead, the data is saved among the network in different nodes, based on attributes of the data. Take the wildlife tracking example for instance: one location of the WSN will store all the information found by the nodes regarding large animals (elephants, hippos), while another location stores everything about birds. If a park manager wants to know something about a certain type of animal, he will have to go to the location related to that type of animal to request the information. When a node senses an animal of a certain type, then it sends the event report to the node where the information about that animal is stored.

Gateway - collecting: A sink can also have a gateway function in which it sends the data to another server that can be queried directly by the user. The gateway function of a sink can also be realized in such a way that users can send queries directly to the sensors. Other setups involve a sink of which the data has to be collected by someone or something else at the sink.

Mobile sink - static sink: Sinks are sometimes mobile, but most literature that we have used for this thesis is based on the assumption that the sink is static and remains at one position.

Mobile nodes - static nodes: A WSN its nodes can be static, but also mobile. A static node does not move from its current position, while a mobile node can move from one position to another. When the nodes are mobile, then the WSN is sometimes called a mobile WSN.

Hierarchical - flat: A WSN its logical topology can either be organized as a flat structure or as a hierarchical structure. In a flat logical topology, all nodes are equal. Nodes send their reports via intermediary nodes towards the sink and there is no appointed set of intermediary nodes that should always take care of forwarding the reports of others. In an hierarchical logical topology, nodes are often organized in a tree topology. A node then has to forward reports from other nodes or aggregate reports from other nodes and report it to its parent node.

Homogeneous - heterogeneous: Some WSNs are homogeneous in the sense that all nodes, but the sink, are equal: they have the same hardware platform, operating system and all use the same power source. Other WSNs are heterogeneous: they use different nodes within the WSN.

II. RELATED WORK

Yun Li and Jian Ren et al.[3] Wireless sensor networks (WSNs) have the potential to be widely used in many areas for unattended event monitoring. Mainly due to lack of a protected physical boundary, wireless communications are vulnerable to unauthorized interception and detection. Privacy is becoming one of the major issues that jeopardize the successful deployment of wireless sensor networks. While confidentiality of the message can be ensured through content encryption, it is much more difficult to adequately address the source-location privacy. For WSNs, source-location privacy service is further complicated by the fact that the sensor nodes consist of low-cost and low-power radio devices, computationally intensive cryptographic algorithms and large scale broadcasting-based protocols are not suitable for WSNs. In this paper, we propose source-location privacy schemes through routing to randomly selected intermediate node(s) before the message is transmitted to the SINK node. We first describe routing through a single a single randomly selected intermediate node away from the source node. Our analysis shows that this scheme can provide great local source-location privacy. We also present routing through multiple randomly selected intermediate nodes based on angle and quadrant to further improve the global source location privacy. While providing source-location privacy for WSNs, our simulation results also demonstrate that the proposed schemes are very efficient in energy consumption, and have very low transmission latency and high message delivery ratio. Our protocols can be used for many practical applications.

Jian Ren Yun Li Tongtong Li et al [4] Wireless sensor networks (WSN) have the potential to be widely used in many areas for unattended event monitoring. Mainly due to lack of a protected physical

boundary, wireless communications are vulnerable to unauthorized interception and detection. Privacy is becoming one of the major issues that jeopardize the successful deployment of wireless sensor networks. While confidentiality of the message can be ensured through content encryption, it is much more difficult to adequately address the source-location privacy. For WSN, source-location privacy service is further complicated by the fact that the sensor nodes consist of low-cost and low-power radio devices, computationally intensive cryptographic algorithms (such as public-key cryptosystems) and large scale broadcasting-based protocols are not suitable for WSN. In this paper, we propose a scheme to provide both content confidentiality and source-location privacy through routing to a randomly selected intermediate node (RRIN). While being able to provide source-location privacy for WSN, our simulation results also demonstrate that the proposed scheme is very efficient and can be used for practical applications.

Yun Li, Jian Ren et al [5] Wireless sensor networks (WSNs) have been widely used in many areas for critical infrastructure monitoring and information collection. While confidentiality of the message can be ensured through content encryption, it is much more difficult to adequately address source-location privacy (SLP). For WSNs, SLP service is further complicated by the nature that the sensor nodes generally consist of low-cost and low-power radio devices. Computationally intensive cryptographic algorithms (such as public-key cryptosystems), and large scale broadcasting-based protocols may not be suitable. In this paper, we first propose criteria to quantitatively measure source-location information leakage in routing-based SLP protection schemes for WSNs. Through this model, we identify vulnerabilities of some well-known SLP protection schemes. We then propose a scheme to provide SLP through routing to a randomly selected intermediate node (RSIN) and a network mixing ring (NMR). Our security analysis, based on the proposed criteria, shows that the proposed scheme can provide excellent SLP. The comprehensive simulation results demonstrate that the proposed scheme is very efficient and can achieve a high message delivery ratio. We believe it can be used in many practical applications.

Lin Yao, Lin Kang, Pengfei Shang, Guowei Wu et al [6] Wireless sensor networks (WSNs) are widely deployed to collect data in military and civilian applications today. Due to the open nature of a WSN, it is relatively easy for an adversary to eavesdrop and trace packets in order to capture the receiver. Therefore, location privacy, particularly the location privacy of the sink node, requires ultimate protection because of its critical position in WSNs. In this paper, we propose a sink location privacy protection scheme by injecting fake packets, but every real packet is still routed along its shortest path. The fake packets are routed to some random destinations and some fake sinks in order to provide the path diversity. It is difficult for an attacker to distinguish the real packets from the fake packets. Thus, the chance of finding the real sink by packet-tracing attack is reduced. Privacy analysis shows that the sink location privacy can be protected better with higher successful probability. We examine the packet travel delay, safe time, and energy consumption by both mathematical analysis and simulations.

Wuchen XIAO, Hua ZHANG, Qiaoyan WEN, Wenmin LI et al [7] Source location privacy is one of the most challenging issues in WSN applications. Some of existing solutions defend the leakage of location information from a limited local adversary who can only observe network traffic in small region, while the global adversary can monitor the entire network traffic. Meanwhile, most of the previous works ignore the categories of RFID. In this paper, we propose a scheme named General Fake Source (GFS) against a global adversary. It supports the passive RFID, which has no battery, cannot send a signal actively. Through simulations, we show that GFS well unifies the behavior of real and fake data sources and provides trade-offs between privacy and energy consume for source location privacy in WSN.

III. PROPOSED METHODOLOGY

Intrusion detection is the major task in networking. There are so many solution provided by the researchers for the detection of intruder in the network. Like Pattern Matching, Measure Based method, Data Mining method and Machine Learning Method.

Here we are using TPP technique for the purpose of Intrusion Detection. TPP technique will be applied by using DH. Using DH we will generate authentication key for every node in the existing network. So before transferring the packet the source node will check the authentication key of the destination node and if the key is correct then only the packet will be transferred and if the key is incorrect that node will be detected as intruder. So this system will help us to identify the misbehavior node in our system when any data, text or packet is transferred. For the security of the packet we are encrypting the packet by using Blowfish Algorithm. In Fact various IDS in MANET uses acknowledgment- based scheme like AACK or 2ACK, but the functionality of such system depends on the acknowledgement packet. Thus, it is very important to ensure that the acknowledgment packet is authenticated. Hence, we adopt proposed architecture which includes digital signature i.e. (EAACK enhanced AACK).

System Assumptions

- The networks are evenly divided into small grids. The sensor nodes in each grid are all fully connected. In each grid, there is one header node responsible for communicating with other header nodes nearby. The whole networks are fully connected through multi-hop communications.
- The information of the SINK node is public. It is the destination that all data messages will be transmitted to through multi-hop routing.
- The content of each message will be encrypted using the secret key shared between the node/grid and the SINK node. However, the encryption operation is beyond the scope of our proposed system.
- The sensor nodes are assumed to have the knowledge of their adjacent neighboring nodes.
- Signal strength of the fake sources are greater than the real source.

Adversary Assumptions

We assume that there are some adversaries in the target area, who try to locate the source node through traffic analysis and tracing back.

- The adversaries will have unbounded energy resource, adequate computation capability and sufficient memory for data storage. The adversaries may also compromise some sensor nodes in the networks.
- The adversaries will not interfere with the proper functioning of the networks, such as modifying packets, altering the routing path, or destroying sensor devices, since such activities can be easily identified. However, the adversaries may carry out passive attacks, such as eavesdropping the communications.
- The adversaries are able to monitor the traffic in an area and get all of the transmitted messages. On detecting an event, they could determine the immediate sender by analyzing the strength and direction of the signal they received. However, we assume that the adversaries are unable to monitor the entire WSNs.

A. Fake Packet Injection

Routing with Fake Sources Baseline flooding and single-path routing cannot provide privacy protection because the adversary can easily identify the shortest path between the source and the sink. This behavior may be considered a result of the fact that there is a single source in the network, and that messaging naturally pulls the hunter to the source. This suggests that one approach we can take to alleviate the risk of a source-location privacy breach is to devise new routing protocols R that introduce more sources that inject fake messages into the network. In order to demonstrate the effectiveness of fake messaging, we assume that these messages are of the same length as the real messages, and that they are encrypted as well. Therefore, the adversary cannot tell the difference between a fake message and a real one. As a result, when a fake message reaches the hunter, he will think that it is a legitimate new message, and will be guided towards the fake source. One challenge with this approach is how to inject fake messages. We need to first decide how to create the fake sources, and when and how often these fake sources should inject false messages. Specifically, we want these fake sources to start only after the event is observed, otherwise the use of fake sources would consume precious sensor energy although there is no panda present to protect.

B. Key Generation Using D-H Algorithm

Diffie–Hellman key exchange (**D–H**)

D-H is a cryptographic that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

Synonyms of Diffie–Hellman key exchange include [:

- Diffie–Hellman key agreement
- Diffie–Hellman key establishment
- Diffie–Hellman key negotiation
- Exponential key exchange
- Diffie–Hellman protocol

IV. RESULT AND EVALUATION

Our Implementation consists of fix number of nodes and used Diffie Hellman algorithm to generate to actual nodes. Firstly we initialized all nodes in network with fake node also than all nodes traverse throughout the network with fake nodes. All nodes contain sink and source node address but in encrypted form except fake node.

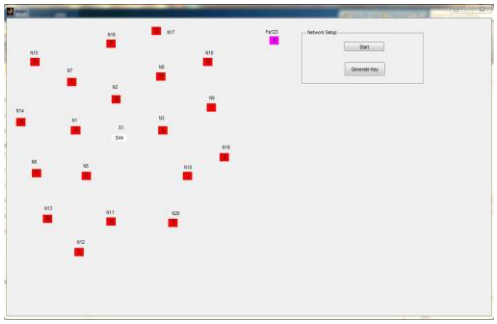

Fig2: initialized nodes

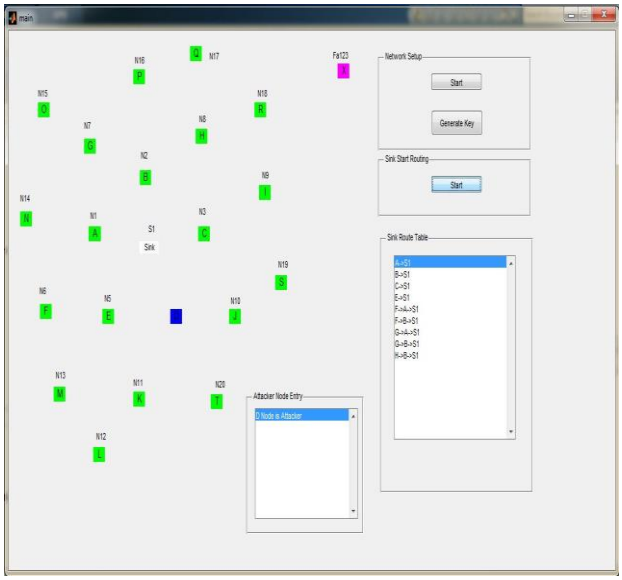

Fig3: Hide source node

Below output show key generation for nodes by Diffie Hellman algorithm

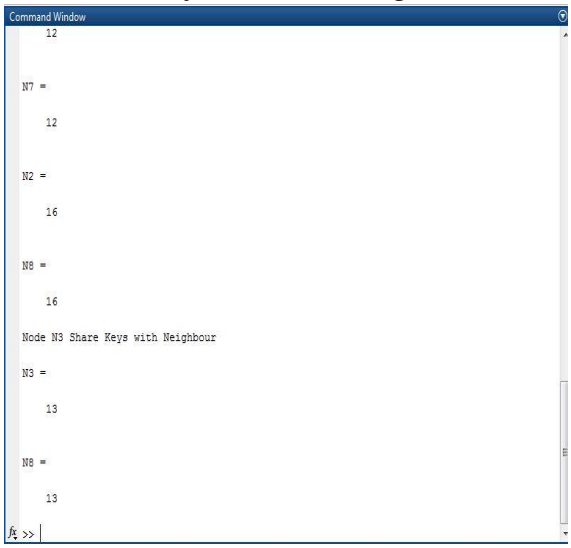

Fig4: Key Generation

V. CONCLUSION

Providing privacy for contextual information such as location of the source or sink node is very important in sensor network. An adversary can use location information and perform some attacks on either source node or destination node. In this paper, we have proposed Intrusion detection is the major task in networking. There are so many solution provided by the researchers for the detection of intruder in the network. Like Pattern Matching, Measure Based method, Data Mining method and Machine Learning Method.

Here we are using TPP technique for the purpose of Intrusion Detection. TPP technique will be applied by using DH. Using DH we will generate authentication key for every node in the existing network. So before transferring the packet the source node will check the authentication key of the destination node and if the key is correct then only the packet will be transferred and if the key is incorrect that node will

be detected as intruder. So this system will help us to identify the misbehavior node in our system when any data, text or packet is transferred. For the security of the packet we are encrypting the packet by using Blowfish Algorithm. In Fact various IDS in MANET uses acknowledgment- based scheme like AACK or 2ACK, but the functionality of such system depends on the acknowledgement packet. Thus, it is very important to ensure that the acknowledgment packet is authenticated. Hence, we adopt proposed architecture which includes digital signature i.e. (EAACK enhanced AACK) .

REFERENCES

[1] Akyildiz IF , Su W , Sankarasubramaniam Y, Cayirci E (2002) Wireless sensor networks: a survey. Comput Netw 38(4):393–422

[2] Li N , Zhang N , Das SK , Thuraisingham B (2009) Privacy preservation in wireless sensor networks: a state-of-the-art survey. Ad 7(8):1501–1514. doi:10.1016/j.adhoc.2009.04.009

[3] Yun Li and Jian Ren , " Source - Location Privacy through Dynamic Routing in Wireless Sensor Networks", publication in the IEEE INFOCOM 2010 proceedings

[4] Jian Ren, Yun Li, Tongtong Li, "Routing-Based Source-Location Privacy in Wireless Sensor Networks", publication in the IEEE ICC 2009

[5] Yun Li, Jian Ren, " Quantitative Measurement and Design of Source - Location Privacy Schemes for Wireless Sensor Networks" , IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 7, JULY 2012

[6] Lin Yao, Lin Kang, Pengfei Shang, Guowei Wu, " Protecting the sink location privacy in Wireless sensor networks" , Received: 18 September 2011 / Accepted: 29 December 2011 Published online: 28 April 2012, Springer-Verlag London Limited 2012

[7] Wuchen XIAO, Hua ZHANG, Qiaoyan WEN, Wenmin LI, "PASSIVE RFID-SUPPORTED Source Location Privacy Preservation Against Global Eavesdroppers in WSN", Beijing University of Posts and Telecommunications, Beijing 100876, P. R. China, Proceedings of IEEE IC-BNMT2013

