Proficient Techniques and Protocols for the Identification of Attacks in WSN: A Review

Preeti Sharma* and Gaurav Gupta
School of Electrical and Computer Science Engineering, Shoolini University Bhajol, Solan - 173229, Himachal Pradesh, India; preetisharma@shooliniuniversity.com, gaurav@shooliniuniversity.com

Abstract

Objectives: In WSN (Wireless Sensor Network) attacks are the central concern. In this paper, we discuss various authentication techniques and protocols for detection of attacks in WSN). Our scope be situated on the way to take new authentication technique by analyzing various techniques and protocols for detection of attack. This technique solves the problems in existing techniques like micro Timed Sufficient Streaming Loss Tolerant Authentication protocol (µ TESLA), Secured Network Encryption Protocol (SNEP), Long Term Equity Anticipation Security (LEAP) ad node authentication all these techniques require an extra amount of energy for computational cost is very high. Analysis: Wireless Sensor Network (WSN) is used in various applications to monitor the sensitive environment. These applications have a high impact in human pursuit, battlefield monitoring and surround watching. After the deployment of the sector nodes at respective places the manual maintenance and monitoring is minimum for long interval of time due to these conditions it creates security problems at sensitive areas wherever the appliance is deployed. In this environment anyone will comes within the network to modify and hack the data. Due to this reason interference of the network also suffers from several constraints like low computation capability and restricted energy. These constraints conjointly build a security as a challenge in Wireless Sensor Network. In this paper we have various security protocols and techniques to beat these problems. Findings: By the limitations of resource we analysis and find the Zero Knowledge Protocol with Interlock Protocol for Sybil attack detection in WSN. These techniques having a less bandwidth, small computational power and less memory space.

Keywords: Group Key Management, Long Term Equity Anticipation Security (LEAP), Micro Timed Sufficient Streaming Loss Tolerant Authentication Protocol (µ TESLA), Wireless Sensor Networks (WSN), Zero Knowledge Verification Protocol

1. Introduction

WSN is more demanding and rising research domain in our real time. A WSN is a group of independent nodes, which communicates in wireless medium with limited frequency and bandwidth consumption. The constraints and different operations in open and hash environment, the security and secrecy which are considered as very exceptionally difficult problems in WSN. Sensor hubs are utilized to assemble sensor system have confinements in term of assets, for example, storage and computation capabilities. In WSN many sensor networks have mission-basis undertakings require that security for dishonorable utilization of data or utilizing produced data may bring about undesirable data spillage and give mistaken results.

In previously various attacks like warm-hole, Sybil, sinkhole and hello flood are detected in the network by different types of techniques and protocols. Due to various types of attacks security is the main problem in WSN. We focus on Sybil attack previous techniques for detection of attack are nodes can be verify the Sybil identities with other identities such as

- Sybil attack would be a major attack in this attack one node has multiple identities. This fake node act as a sender, it will send false information to its neighbors and receiver, it will receive the information that is originally destined for a legitimate node and consumes a lot of energy. This problem is overcome by Sybil secure is projected. Sybil Secure consumes less energy than existing defense mechanisms.

* Author for correspondence
• Radio asset testing key approval, area confirmation and enlistment. The most encouraging system among these that the irregular key pre-dispersion which assistant a hub’s keys with its character. In these techniques radio resource verification breakable in some-times such as radio hardware and price of validation is costlier. In position verification an attacker can generate verify nodes position.. This drawback is overcome by Receives Signal Strength (RSSI). These schemes have a strong solution.

• Identifying and Preventing Sybil Attacks in WSN exploitation Message Authentication and spending technique. The current methodology Random Password Comparison (RPC) has exclusively scheme that basically checks the hub personalities by investigating the neighbors. This problem is resolved by the combined CAMPVM (Compare and Match-Position Verification Method) with MAP (Message Authentication and Passing) for distinguishing, dispensing, and in the end keeping the passage of Sybil nodes within the network.

• Another technique for detection of attack is using neighboring node messaging that means time to time messages. This method gives the higher potency in terms of detection of speed and time. So it will take extra time for computation.

• All these issues for detecting Sybil attack is overcome by another protocols that is Zero data Protocol2,3. Zero Knowledge (ZKP) is combined with interlock protocol and µ TESLA protocol take less time, energy and give better output as compare to these existing techniques. This can create secure network against Sybil attack.

2. Materials and Methods

Sybil Attack having a malevolent hub exhibit numerous characters to the system is called Sybil attack. This attack is particularly confusing to geographic routing protocols as the adversary appears to be in various areas without a moment’s delay. In Wireless Sensor Networks (WSN) a Sybil attacker4,5 can change the aggregated analysis of outcome by acting or subsidizing many times as a different nodes. This attack can disrupt varied operations of the wireless networks like data group and routing mechanisms. This attack is simulated by Network Simulator-3 (NS-3).

2.1 Tool Selection

• NS-3 Simulator: NS-3 is a free, open source software project building and maintaining a discrete-event network simulator for research and education. It help to improve the technical rigor of network simulation practice. NS-3 written in C++ with bindings available for python. NS-3 is a GNU GPLv2-licensed project. NS-3 provides the feature not available in NS-2 simulator.

• Programs in NS-2 area unit written in Object orientated extension of Tcl (OTcl) and results of simulations may be pictured victimization the Network Animator (NAM). It’s unacceptable to run a simulation in ns-2 strictly from C++ (i.e., as a main () program with none OTcl). Moreover, some parts of ns-2 area unit written in C++ et al., in OTcl. In NS-3, the machine is written entirely in C++, with optional Python bindings. Simulation scripts will thus be written in C++ or in Python. New animators and visualizers area unit on the market and underneath current development.

• The total computation time required to run a simulation scales better in NS-3 than NS-2.

3. Results and Discussions

3.1 µ TESLA

µ TESLA protocol6 is based on the distribution of packets. Uneven digital signatures square measure unreasonable for sensing element networks for the authentication, as they need the long signatures with high communication. However, TESLA wasn't designed for sensing element network projected small regular enough streaming loss tolerant authentication µ TESLA is to resolve the subsequent lacks of TESLA in sensing element network:-

• TESLA authenticates the initial packet with a digital signature that is that the big-ticket for our sensing element nodes.
• Disclosing a key in every packet needs an excessive amount of energy for causing and receiving µTESLA leak the key once per epoch.
• µTESLA restricts the number of authenticates senders.
• No digital signatures are used to initial to initially authenticate.
3.2 SNEP
SNEP stand for Secured network encryption protocol has pair of substances base station and ace for generation of keys. Every hub imparts a couple of key to base station and option keys square measure acquired from ace. It is frightfully useful convention that ensures protection and integrity. SNEP have some properties:
- Semantic security: The counter price is incremented once every message, an equivalent message is encrypted otherwise, when the counter price is long enough that it ne'er repeats at intervals the life of node.
- Data authentication: If the Medium Access Control (MAC) verifies properly, the receiver is assured that the message originated from the claimed sender.
- Replay protection: The counter price within MAC prevents replaying recent messages. If the counter weren't available in the MAC, an adversary could be easily replay messages.
- Weak freshness: If the message verified properly, the receiver is alert to that the message ought to square measure sent once the previous message is received properly that had a lower counter value.
- Low communication overhead: The counter state is unbroken at every finish purpose and doesn't have to be compelled to be sent in every message.

3.3 LEAP
Long Term Equity Anticipation Security (LEAP) is used for information change theme where hubs having fully totally diverse security desires. The degrees of keys square measure personal keys mix of keys between nodes and cluster keys.

3.4 User Authentication
In this authentication any user must exchange information with device hubs. The user give a signed request to totally different device hubs and thus the hubs confirm the request primarily which is based upon ID of the hub. Once flourishing confirming a session secret is produced between device hub of system and user. User will give the encrypted queries and notice access to information. Resulting issues will suffer from the highest of the schemes.

3.5 Node Authentication
The enormous facts of device hubs unit mounted and once sent there is no manual support and perception till future. Because of this situation it makes a security inconvenience. Node, ten unit loads of on the substance of it to be packed with different physical attacks that additional cause hub compromise, hub look into venture, man-in-middle attack and replay attack. Stack of analysis unit pulled in towards the assurance of wireless device system as an aftereffects of until no solid mechanism is set up all through this event. The principle to this is asset limitation and appropriate unattended surroundings of device systems and unattended environment.

3.6 Results
The results comes by of these discussion like in small regular decent streaming loss tolerant authentication (µTESLA) needs long signatures with high communication overhead of approx fifty upto1000 bytes.
- Secured Network Cryptography Protocol (SNEP) has low communication overhead because it adds solely 8 bit per message.
- In User Authentication the verification of nodes is incredibly slow.
- Various senders can't broadcast at the constant time.
- Late authentication caused Denial of Service (DoS) attack.
- Performance isn't up to mark for giant scale networks.
- Powerful senders are required.
- Node Authentication the preparation of detector system is typically in setting which could be harmful with physical attacks. Wireless medium don't alter ancient private techniques that unit of measurement best fitted to wire medium.

4. Conclusion and Future work
Attacks are the main issue in wireless sensor network. Many protocols and techniques are used for detection of attacks in WSN. In this paper we discussed various existing techniques and protocols for detection of attacks. So, we propose the Sybil attack detection by using ZKP.
(zero knowledge protocol) with Timeout-Mac (T-Mac) protocols. By this technique Zero data Protocol (ZKP) have a less machine value as there aren’t any high calculations needed. So, this can scale back the energy and storage necessities of the device node. And additionally Timeout-Mac (T-Mac) handles the traffic fluctuations. This conserves the energy by preventing Sybil attack in Wireless device Network (WSN).

The main target in WSN is to secure the authentication techniques and protocols against the malicious nodes to hide the unwanted packets transmission to scale back the energy loss and to urge eliminate attacks and will increases the data delivery ratio. It suggested that extra analysis on hierarchical information aggregation approaches for heterogeneous nodes ought to be conducted for existing protocols.

5. Acknowledgement

I glad to my guide Mr. Gaurav Gupta who helping me in my research work and also thankful to Dr. Varun Jaiswal who guided me and solve all types of problem related to my research work.

6. References

1. Naik S, Shekokar N. Conservation of energy in wireless sensor network by preventing denial of sleep attack. Procedia Computer Science. 2015; 45:370–9.
2. Kilian J, Micalli S, Ostrovsky R, editors. Minimum resource zero knowledge proofs. IEEE 30th Annual Symposium on Foundations of Computer Science; Research Triangle Park. 1989. p. 474–9.
3. Anh B, Huy P, editors. A zero-knowledge protocol based on a new product of durations. IEEE International Symposium on Signal Processing and Information Technology (ISSPIT); 2012. p. 1–6.
4. Demirbas M, Song Y, editors. An RSSI-based scheme for sybil attack detection in wireless sensor networks. Proceedings of the International Symposium on on World of Wireless, Mobile and Multimedia Networks; IEEE Computer Society. Buffalo-Niagara Falls. 2006. p. 564–70.
5. Vasudeva A, Sood M. Sybil attack on lowest id clustering algorithm in the mobile ad hoc network. International Journal of Network Security and its Applications. 2012; 4(5):135.
6. Karlof C, Wagner D. Secure routing in wireless sensor networks: Attacks and countermeasures. Ad hoc networks. 2003; 1(2):293–315.
7. Ramesh P, Femi P, Santhi B. Review on Security Protocols in Wireless Sensor Networks. Journal of Theoretical and Applied Information Technology. 2012; 38(1):1–4.
8. Boyle D, Newe T. Securing wireless sensor networks: Security architectures. Journal of Networks. 2008; 3(1):65–77.
9. Dhawale SD, Hogade B, Patil S. Design and Implementation of a Dynamic Key Management Scheme for Node Authentication Security in Wireless Sensor Networks. IJSETR. 2005; 4(4):1–4.
10. Khan WZ, Aalsalem MY, Saad MNBM, Xiang Y. Detection and mitigation of node replication attacks in wireless sensor networks: A survey. International Journal of Distributed Sensor Networks. 2013; 2013:22.