A Review on Authentication and Security Maintenance in Wireless Sensor Network

Dr.P.Maxmillon, R.Franklin
Department of Computer science,
Sri Krishnadevaraya University, Anantapur

Abstract

Wireless sensor networks (WSN) are charity to scrutinize and to sustain the physical orconservational conditions like temperature, sound, pressure, etc. and exploited to pass theinformation through the network to a central location. The wireless networks are bi-directional thatassistances in controlling and preserving the sensor activities. Wireless sensor networks are charity inmany security attacks with false data injection, data forgery, and hearing. A large sensornetwork with the discrete sensor nodes aims on security factor. A node injected into the sensornetwork for the data forwarding results in several attacks. These attacks are outcomes in theinoculation of false data in the wireless sensor network. In a huge scale wireless sensor network,perceiving reports injected by co-operated nodes is a large research confront. If a node isconjoined, all the security information collects the nodes are turns out to be reachable to theattacker. In order to increase the maintenance and security level in the wireless sensor networks,authentication system is designed. In this authentication system, the sanctuary maintenance level is increased by cleaning the false data. The wireless sensor networks aims on removing the injected false data attack and the moderation technique is designed for high security maintenance. The riddling false data are executed earlier to ease the system with the high security. Our enquiry work aims to increase the security and maintenance level in the wireless network.

I. INTRODUCTION

Wireless Sensors Network (WSN) authentication is aincreasing technology consequential from progress of different fields for diminishing the false data attacks. In wireless sensor networks, sensor nodes introduce false data throughout both data aggregation and data forwarding. The false data detection method takes false data injections during data forwarding and fails to certification alterations on the data by data aggregation. Many applications of wireless sensor networks (WSNs) be contingent on data about the positions of sensor nodes. The central aim of the routing protocols in sensor networks is the controlled ability of the nodes and the application of the exact nature of the networks to increase the sanctuary. Wireless sensor networks (WSNs) are used in unfocused atmosphere where the energy replacement is a complex one. Since of the inadequate resources, a WSN requirements to satisfy application specific QoS desires and to reduce the energy consumption to extend the system lifetime and security maintenance. Wireless sensor networks (WSN) increased various research activity because of the exciting and resounding reasons offered by the potential for imperative monitoring submissions on dissimilar subjects. The main aim of the sensor network is to distinct tiny sensing devices that are capable of sensing alterations of incidents or parameters and equivalent with other devices over a particular geographic area for board tracking, surveillance, environmental monitoring etc.

Security is working from surrounding the features of authentication, integrity, privacy, non-repudiation, and anti-playback. Wireless Sensor Networks (WSNs) is network contains of sensor nodes or motes collaborating wirelessly with each other for improving the security level. Expansion in sensor, low power processor, and wireless communication knowledge aimed to the broad utilization of WSNs functions in modern world like broadcast substantiation. Broadcast authentication is an indispensible and important security mechanism in a WSN since broadcast is a natural communication method in a wireless environment. When base stations need to send commands to thousands of sensor nodes, broadcasting is more resourceful technique than unicasting to each node. Broadcast authentication is a security service in wireless sensor networks (WSNs) that authorizations the mobile users of WSNs to broadcast messages to multiple sensor nodes in a protected way. The authentication and security maintenance process in wireless sensor network aims to:

- To accomplish high effective bandwidth technique on reducing the gang injecting false data attack
- To augment the authentication scheme on sensor network by overcoming the false data injection
- To conserve the system with high authentication scheme without any false data injection

II. ANALYSIS OF EXISTING LITERATURE

Wireless Sensor Networks (WSN) contains large number of supply limitations for sensor nodes in some applications. Bandwidth-efficient cooperative authentication (BECAN) scheme riddles the inserted false data in wireless sensor network. BECAN accrue energy by filtering the majority of inserted false data with minor extra overheads at the en-route nodes. But, BECAN fails to avoid/moderate the gang injecting the false data attack from mobile negotiated sensor nodes. The Data Aggregation and Authentication protocol (DAA) combines false data detection. Categorises the false data interleaved by a data aggregator for reducing the misuse of resources like bandwidth and battery power. Each sensor node can able to aggregate and forward data but fails to enhance the network security and efficiency. Network Security architecture with ticket based protocol reassures the anonymous access control. It changes the hierarchical identity-based cryptography (HIBC) for inter province authentication. Client's bandwidth allocation depending on the logged data is not effective in sensor network.

Security Games for Node Localization using probabilistic approach selects the repetition of the nodes. Game theoretical condition for WSNs is verifiable multi-literation is used though additional security counter calculates are taken place. Malicious node's max-min strategy consequential in the optimal strategy is not evidenced in wireless sensor network. Virtual Energy-Based Encryption and Keying (VEBEK) scheme is a secure communication framework someplace sense data is tutored using a variation code created through the RC4 encryption mechanism. RC4 encryption alters function of the lingering virtual energy of the sensor but threats on dynamic paths transpired. Distributed Token Reuse Detection (DTRD) scheme for Privacy-Preserving Access Control for sensor network purchase the tokens from the network owner. Proficient DTRD techniques for Distributed Privacy-Preserving Access Control scheme (DP2AC) under changed attacker model are not studied. Virtual Ring Architecture as demonstrated, it offers privacy fortification in the smart grid situation with cost efficient factor. New security mechanisms are not maintained with future resource computing environments in wireless sensor network.

Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks uses outstanding design constraint settings at runtime due to environment alterations. Multipath route decision intrusions take place in sensor network system. Sequential mOnte carLo combIned with shadow-faDing estimation (SOLID) method follows the small scale prime data transferring. The main aim is to increase the temporal shadow fading connexion in sensing results induced by the primary user's mobility. Signal propagation was more accidental, the attack takes place in system with cruel adversaries on data forwarding.

Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks usesexceptional design constraint situations at runtime due to atmosphere alterations. Multipath route decision intrusions take place in sensor network system. Sequential mOnte carLo combIned with shadow-faDing estimation (SOLID) process follows the small scale primary data transferring. The central aim is to increase the temporal shadow fading correlation in sensing results induced by the major user's mobility. Signal propagation was more random, the attack takes place in system with cruel oppositions on data forwarding.

A. Security Games for Node Localization through Verifiable Multilateration:

Node localization is momentous in wireless sensor network (WSN) applications. Location is working to enhance the routing and saving power and to enterprise applications where services are location reliant. A method is used to figure node reputation and the related accuracy of the monitored data is compulsory. Definite approach is employed to limit nodes when few are collaborated and it is called as Verifiable Multilateration (VM). VM estimates an unknown position by leveraging on a set of important landmark nodes called as verifiers. VM can also able to identify reliable localization actions and definite cruel performances. Multilateration is the most important technique employed in WSNs to estimate the coordinates of unknown nodes specified by the positions of landmark nodes christened as anchor nodes whose positions are identified. The position of unknown node is premeditated by geometric inference based on the distances among the anchor nodes and the node. Though, malicious node's maxmin strategy resembles to the optimal strategy is not proved. It fails to outspread the framework to handle multiple malicious nodes. Supplementary security counter measures are not carried out in this process.

B. Design and Performance Analysis of a Virtual Ring Architecture for Smart Grid Privacy:

Virtual ring architecture is intended to ensure privacy defence of smart grid users. The virtual ring forms a network of smart meters going to the same geographical region. For forecasting purposes, the energy supplier fails to know the energy consumption of aindividual smart meter than the total energy ingestion of a particular geographical region. The shrewd meters of the same virtual ring share the associated pair of keys that contains a public key and a private key. The virtual ring's key pair is the pair of keys twisted by the energy provider and increased on every smart meter of a particular virtual ring. In place

of containing a set of neighbours, every smart meter in a particular virtual ring has only two neighbours – a clockwise one and an anticlockwise one. Each smart meter in the ring take cares the receiving data from its downstream neighbour and sending data to its upstream neighbour. The upstream/downstream neighbours of aindividual smart meter are not desirable for the closest two neighbours to the specific smart meter. All smart meter contains a copy of the energy supplier certificate. The energy supplier attaches to any smart meter to revolutionize the upstream/downstream neighbours of a particular smart meter. Each virtual ring contains an identifier (IDVR*)*. However, new security mechanisms are not maintained with future resource computing environments.

C. Integration of False Data Detection with Data Aggregation and Confidential Transmission in Wireless Sensor Networks:

Wireless sensor networks are unprotected to security attacks with false data injection, data forgery, and snooping. Sensor nodes cooperated by intruders, and the cooperated nodes alter data integrity by implanting the false data. The transmission of false data reduces the constrained battery power and alters the bandwidth usage. False data are inoculated by negotiated sensor nodes in many ways with data aggregation and relaying. As data aggregation is substantial to minimize data redundancy and/or to increase the data accuracy, false data detection is significant to the condition of data integrity and proficient usage of battery power and bandwidth. Data discretion chooses data to be encrypted at the source node and decrypted at the destination. But, key establishing process is more defenceless to node compromise attacks. False data detection and data discretion increase the communication overhead. Every sensor node is capable of both collecting and forwarding data but does not improve network security and efficiency.

D. SAT: A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks:

The wireless mesh backbone consists of mesh routers (MRs) and gateways (GWs) connected by shared wireless links. Mesh routers and gateways serve as the access points of the WMN. The hospital, campus, enterprise, and domestic buildings are specimens of individual WMN domains promising to the Internet services from upstream service providers.

III. COMPARISON OF AUTHENTICATION AND SECURITY MAINTANANCE

In order to associate the authentication and security maintenance in wireless networks, amount of users is taken to implement the experiment. The first recital metric is processing time, which is defined as the amount of time required to authenticate and maintain the security level of the user data. The second presentation is false positive rate, which is distinct as amount of malicious users detected while authenticating the user's details. The third performance is security level which is distinct as level of privacy given to the user's data from other user. The fourth performance is the energy feasting which is defined as the amount of energy expended while authenticating and maintaining the security of the user's data.

IV. DISCUSSION ON LIMITATION OF AUTHENTICATION AND SECURITY MAINTANANCE

In probabilistic approach, malevolent node's maxmin strategy matches to the optimal strategy is not proved. The method fails to extend the framework to handle multiple malicious nodes. Supplementary security counter measures are also not carried out in the probabilistic approach. In Data Aggregation and Authentication protocol (DAA), key founding process is more vulnerable to node cooperation attacks. False data detection and data discretion enhances the communication overhead. All sensor nodes can able to aggregate and forward data but does not improve network security and efficiency. Virtual ring architecture fails to support the secrecy protection mechanism with future resource computing environments. Network Security Architecture with ticket based protocol; client's bandwidth allocation dependent on the logged data in log is not real in sensor network. Many threats are occurred on the dynamic paths on Virtual Energy-Based Encryption and Keying (VEBEK) scheme. Distributed token reuse detection (DTRD) scheme for DP2AC under dissimilar attacker model is not inspected. In Mean Time To Failure (MTTF) Probabilistic system cruel attacks materialise with the packet dropping in sensor network. Also the multipath route conclusion intrusions take place in system. In Sequential mOntecarLo combIned with shadow-faDing estimation (SOLID) method, signal proliferation is random and so the attack takes place in the system.

V. CONCLUSION

Comment about the prevailing authentication and security maintenance in wireless sensor networks such as Data Aggregation and Authentication (DAA) protocol, Disseminated token reuse detection (DTRD) Scheme, and Sequential mOnte carLo combIned with shadow-faDing estimation (SOLID) method. Probabilistic approaches regulate the status of the nodes and minimize the maximum deception of the malicious node. Malicious node is attentive to variation the positioning strategy in the attempt to masquerade itself. In Virtual ring architecture, privacy protection solution aims to provision all the aforementioned architectural design

goals. Confidentiality of customers minimizes the performance overhead of cryptographic computations. The architecture also offers privacy protection in the smart grid atmosphere. It is also active to support confidential data transmission among two uninterrupted data aggregators to verify the data integrity on the encrypted data. DAA detects false data inoculated by a data aggregator to minimize the waste of resources such as bandwidth and battery power. VEBEK is a secure communication framework where sensed data is encrypted using a scheme based on a permutation code created via the RC4 encryption mechanism. RC4 encryption alters occupation of the residual virtual energy of the sensor. VEBEK apprises keys deprived of exchanging messages for key renewals.

REFERENCES

[1] Rongxing Lu., Xiaodong Lin., Haojin Zhu., Xiaohui Liang, and Xuemin (Sherman) Shen., "BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks," IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. X, NO. X, XX 2010

[2] SuatOzdemir., and HasanÇam., "Integration of False Data Detection With Data Aggregation and Confidential Transmission in Wireless Sensor Networks," IEEE/ACM Transactions ON Networking, VOL. 18, NO. 3, JUNE 2010

[3] Nicola Basilico., Nicola Gatti., MattiaMonga., and Sabrina Sicari., "Security Games for Node Localization through Verifiable Multi-lateration," IEEE Transactions on Dependable and Secure Computing, VOL. 11, and NO: 1, January/February 2014

[4] Jinyuan Sun., Chi Zhang.,Yanchao Zhang., and Yuguang Fang., "SAT: A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks," IEEE Transactions on Dependable and Secure Computing, vol. 8, NO. 2, March-APRIL 2011 L.Devi*et al*, International Journal of Computer Science and Mobile Computing, Vol.4 Issue.5, May- 2015, pg. 53-70

[5] ArifSelcukUluagac., Raheem A. Beyah., Yingshu Li., and John A. Copeland., "VEBEK: Virtual Energy-Based Encryption and Keying for Wireless Sensor Networks," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 9, NO. 7, JULY 2010

[6] Rui Zhang., Yanchao Zhang., and KuiRen., "Distributed Privacy-Preserving Access Control in Sensor Networks," IEEE Transactions on Parallel and Distributed Systems, VOL. 23, NO. 8, August 2012

[7] Hamid Al-Hamadi., and Ing-Ray Chen., "Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks," IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 10, NO: 2, JUNE 2013

[8] Alexander W. Min., and Kang G. Shin., "Robust Tracking of Small-Scale Mobile Primary User in Cognitive Radio Networks," IEEE Transactions on Parallel and Distributed Systems, Vol. 24, NO. 4, April 2013

[9] MohamadBadra., and SheraliZeadally., "Design and Performance Analysis of a Virtual Ring Architecture for Smart Grid Privacy," IEEE Transactions on Information Forensics and Security, Vol. 9, NO: 2, February 2014