Secured Wireless Sensors Network Using Machine Learning Approach

Neha A. Meshram **Dr. V. M. Thakare**

Abstract —**Machine learning inspires many practical solutions that maximize many resource utilization and prolong the lifespan of a network. As wireless sensors network (WSNs) monitor dynamic environment that rapidly changes over time such behavior is either caused by the external factor or by initiated by the system designers. A comparative guide is provided to aid WSN designers to develop suitable machine learning solutions for appropriate application challenges. The security properties of sensors must be known before deploying the intelligent systems on critical infrastructure. This paper provides some steps for generating a comprehensive security model for sensors network as sensors network is not a traditional computing device hence existing security models are not applicable.**

Keywords — **Wireless sensors network,intelligent systems, critical infrastructure.**

I. INTRODUCTION

Multiple autonomous, tiny, low-cost and low-power sensor nodes comprise a wireless sensors network (WSN). The sensors nodes are equipped with various types of sensors such as thermal , acoustic, chemical, pressure, weather and optical sensors which gather information from various nodes and collaborate to forward sensed data to base stations for further processing. WSNs designers have to address common issues related to data aggregation, data reliability, localization, node clustering, energy aware routing, event scheduling, fault detection and security because of the diversity each application must possess its own individual characteristics and requirements, developing efficient algorithm is a challenging task[1]. Many researches are engaged in producing novel design paradigms to address challenges in current network systems inspired by intrinsic appealing characteristics of biological system[2]. Bio-inspired systems play vital role for solving the problem in another domain as biological approaches seem promising as they are capable to self adapt, self heal, self organize in varying environmental conditions, also they are robust. In wireless communication using sensors wide range applications transmit data using multihop which weakens the security strength thus for efficient transfer of data across networks sensors, mobile sinks (MS) are essential components in the operation of many sensor network applications, including data collection in hazardous environment, localized reprogramming, oceanographic data collection and military navigation. In many of the given applications security is important such as authentication and pairwise key establishment between sensor nodes and mobile sinks. A general framework is developed that permits the use of any pairwise key predistribution scheme as its basic component, to provide authentication and pairwise key establishment between sensor nodes and MSs as mobile sink replication attacks can occur due to easily acquiring fraction of network nodes[3]. A general three-tier security framework is cultivated for the study of new security technique based on polynomial pool-based key predistribution scheme. This proposed technique will substantially improve network resilience to mobile sink replication attacks. In the new security framework, a small fraction of the preselected sensors nodes called the stationary access node, act as authentication access points to the network, to trigger the sensor nodes to transmit their aggregated data to mobile sinks[4].

II. BACKGROUND

One way hash function method is used in the machine learning approach also a K-means method is used which is an unsupervised machine learning methods which works on principles of finding structure out of unlabelled data set.

There are a few drawbacks and limitations that should be considered when using machine learning techniques in wireless sensor networks. Some of these are: As a resource limited framework, WSN drains a considerable percentage of its energy budget to predict the accurate hypothesis and extract the consensus relationship among data samples. Thus, the designers should consider the trade-off between the algorithm's computational requirements and the learned model's accuracy. Specifically, the higher the required accuracy, the higher the computational requirements, and the higher energy consumptions. Otherwise, the developed systems might be employed with centralized and resource capable computational units to perform the learning task. Generally speaking, learning by examples requires a large data set of samples to achieve the intended generalization capabilities (i.e., fairly small error bounds), and the algorithm's designer will not have the full control over the knowledge formulation process. Traditional schemes in ad hoc networks using asymmetric keys are expensive due of their storage and computation cost. These limitations make key predistribution schemes the tools of choice to provide low cost, secure communication between sensor nodes and mobile sinks. But the con of three tier security architecture presents the probability of a mobile polynomial being compromised; hence an attacker can make use of the captured mobile polynomial to launch a mobile sink replication attack against the sensor network.

Although machine learning techniques are applied to many applications still further research techniques are required such as:

- Compressive sensing and sparse coding
- Distributed and adaptive machine learning techniques for WSNs

- Resource management using machine learning
- Detecting data spatial and temporal correlations using hierarchical clustering

III. PREVIOUS WORK DONE

Wireless sensors network: security challenges are proposed by the author Asmae BLILAT et al. which shows the Existing literature has proposed the use of computationally inexpensive cryptographic techniques for handling message confidentiality and authenticity in sensors network. The three tier security scheme in wireless sensor networks with mobile sinks is proposed by Amar Rasheed et al. which shows the wireless sensors network, key management problem is an active research area. Eschenauer and Gilgor proposed a probabilistic key predistribution scheme to bootstrap the initial trust between the sensor nodes. The main idea was to let each sensor node randomly pick a set of keys from a key pool before deployment, so that any two sensor nodes had a certain probability of sharing at least one common key. Heena Rathore et al. proposed The Novel approach for security in wireless sensor network using bio-inspirations which detects the trust management systems using Weightings method, Artificial Neural network and Swarm intelligence. A machine approach for identifying and classifying faults in wireless sensors network is proposed by author Ehsan Ullah Warriach et al. Previous work has used HMMs to simply detect variances, a broader use of it by considering the identification and classification of the type of the detected data fault such as stuck-at, offset and gain, and also to identify and classify the system faults that affect the sensor network. Mohammad Abu Alsheikh et al. proposed The Machine learning in wireless sensors network: Algorithms, Strategies and Applications.

IV. EXISTING METHODOLOGY

Wireless sensors network is a network based on multiple low-cost communication and computing devices connected to sensor nodes which sense physical parameters. The symbiotic nature of biological systems results in the valuable knowledge for computer networks. Because of the analogies between network security and survival of human body under pathogenic attacks biologically inspired approaches are interesting. The proposed research work uses biological inspirations and machine learning technique for adding security against threat also to identify the fraudulent nodes, consecutively by deriving inspiration from human immune system it effectively nullify the impact of the fraudulent ones on the network.

At the interface of the real world and digital applications a wealth of new applications is emerging with the advent of low-power wireless sensor networks. A distributed computing platform which measures properties of the real world, formulate intelligent inferences and instrument responses there is a requirement of strong foundations in distributed computing, artificial intelligence, databases, control theory and security. The security properties of sensors must be known before deploying the intelligent systems on critical infrastructure. This paper provides some steps for generating a comprehensive security model for sensors network as sensors network is not a traditional computing device hence existing security models are not applicable. Various security challenges are proposed for overcoming the difference between the computer and the real world.

A statistical approach is developed to detect and identify faults in WSNs which is focused on the identification and the classification of data and system fault types as it is essential to perform accurate recovery actions which experiences collected data prone to be faulty. Faults are due to external and internal influences such as calibration, low battery, environmental interference and sensor aging. Hidden Markov Models (HMMs) method is used to capture the fault free dynamics of an environment and faulty data. The approach is validated using real data obtained from over one month of samples from motes deployed in an actual living lab.

In many wireless sensors network applications mobile sinks (MS) play a very vital role for efficient data accumulation, localized sensor programming and for distinguishing even revoking comprised sensors. For accessing the network there is a need of key pre distribution schemes between sensors nodes and mobile sinks for pairwise key establishment and authentication. This article describes a three tier general framework that permits the use of any pairwise key predistribution scheme as its basic component. Two pools are required for the new framework one for the mobile sink to access the network and the other for pairwise key establishment between the sensors. The authentication mechanism is strengthened between the sensor and the stationary nodes to reduce the damages caused by the stationary access node replication attacks. Mobile sink replication attack offers higher network resilience as compared to the polynomial pool-based scheme.

Machine learning inspires many practical solutions that maximize many resource utilization and prolong the lifespan of a network. As wireless sensors network (WSNs) monitor dynamic environment that rapidly changes over time such behavior is either caused by the external factor or by initiated by the system designers. A comparative guide is provided to aid WSN designers to develop suitable machine learning solutions for appropriate application challenges.

V. ANALYSIS AND DISCUSSION

Using various security challenges such as measuring confidentiality, timing obfuscation, secure aggregation, topology obfuscation, scalable trust management and aggregation with privacy we can secure the nodes by unauthorized access of the confidential data.

Our analytical results indicate that the new security technique makes the network more resilient to both mobile sink replication attacks and stationary access nodes replication attacks compared to the single polynomial pool-based approach.

Factors such as pressure, PIR, acoustic, temperature, humidity and light intensity influence the sensor for fault occurrence which might be external or internal. But to prevent the data and identify faults immediately HMMs method is proposed and the various parameters are considered such as the data fault classification, data fault detection, system fault, system fault classification, system fault detection, calibration, etc. Machine learning methods are able to handle much of this while ensuring efficient resource utilization, mainly bandwidth and power utilization.

VI. PROPOSED METHODOLOGY

The proposed method determines the positions of multiple sink nodes based on the sensor network. The proposed technique will substantially improve network resilience to mobile sink replication attacks is the three-tier scheme along with the some future applications which are still open and need to be developed such as compressive sensing and space coding, distributed and adaptive machine learning techniques for WSNs, resource management using machine learning and detecting data spatial and temporal correlations using hierarchical clustering. In WNS it is essential to remove the malicious nodes without affecting the overall system for which various trust models are developed such as the Weightings method, ANN, Swarm intelligence.

VII. POSSIBLE OUTCOME AND RESULTS

Different machine learning classifiers are used to recognize different types of streams, thus eliminating the need for flow-aware management techniques. The requirements for QoS guarantee, data integrity and fault detection depend on the network service and application. Machine learning methods are able to handle much of this while ensuring efficient resource utilization, mainly bandwidth and power utilization. Hence, a better solution would be to either slowly decreases the sampling interval to zero or to increase the sampling interval depending on the application. Factors such as pressure, PIR, acoustic, temperature, humidity and light intensity influence the sensor for fault occurrence which might be external or internal. But to prevent the data and identify faults immediately HMMs method is proposed and the various parameters are considered such as the data fault classification, data fault detection, system fault, system fault classification, system fault detection, calibration, etc. Using various security challenges such as measuring confidentiality, timing obfuscation, secure aggregation, topology obfuscation, scalable trust management and aggregation with privacy we can secure the nodes by unauthorized access of the confidential data.

CONCLUSION

Machine learning provides a collection of techniques to enhance the ability of wireless sensor network to adapt to the dynamic behavior of its surrounding environment. Studies that have adopted machine learning methods to address these challenges from distinct research areas have been discussed. Moreover, numerous issues are still open and need further research efforts such as developing lightweight and distributed message passing techniques, online learning algorithms, hierarchical clustering patterns and adopting machine learning in resource management problem of wireless sensor network.

REFERENCES

[1]Mohammad Abu Alsheikh, Shaowei Lin, Dusit Niyato, Memebr, IEEE and Hwee-Pink Tan, Senior member, IEEE," Machine learning in wireless sensor networks: Algorithms, Strategies and Applications", IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 16, NO. 4, FOURTH QUARTER 2014

[2] Heena Rathore, Venkataramana Badarla, SDushmita Jha, Anupam Gupta, " Novel approach for security in wireless sensor network using Bio-inspirations", IEEE journal 2014

[3] Amar Rasheed, Student Member, IEEE, and Rabi N. Mahapatra, Senior Member IEEE,'The three- tier security scheme in wireless sensor networks with mobile sinks", IEEE TRANSACTIONS ON PARALLEL AND SITRIBUTED SYSTEMS, VOL. 23, NO. 5, MAY 2012

[4] Ehsan Ullah Warriach, Marco Aiello, Kenji Tei," A machine learning approach for identifying and classifying faults in wireless sensor nertworks", IEEE 15th International Conference on Computational Science and Engineering 2012

[5]Asmae Blilat, Anas Bouayad, Nour el houda Chaoui, Mohammad el Ghazi, " Wireless sensor network: Security Challenges" IEEE taransactions on sensor security 2012

AUTHOR'S PROFILE

Neha A. Meshram has completed B.E. Degree in Computer Science and Engineering from Sant Gadge Baba Amravati University, Amravati, Maharashtra. She is persuing Master's Degree in Computer Science and Information Technology from P.G. Department of Computer Science and Engineering, S.G.B.A.U. Amravati. (e-mailid: meshram.ner@gmail.com)

Dr. V. M. Thakare

Dr. Vilas M. Thakare is Professor and Head in Post Graduate department of Computer Science and engg, Faculty of Engineering & Technology, SGB Amravati university, Amravati. He is also working as a coordinator on UGC sponsored scheme of e-learning and m-learning specially designed for teaching and research. He is Ph.D. in Computer Science/Engg and completed M.E. in year 1989 and graduated in 1984-85.

He has exhibited meritorious performance in his studentship. He has more than 27 years of experience in teaching and research. Throughout his teaching career he has taught more than 50 subjects at various UG and PG level courses. He has done his PhD in area of robotics, AI and computer architecture. 5 candidates have completed PhD under his supervision and more than 8 are perusing the PhD at national and international level. His area of research is Computer Architectures, AI and IT. He has completed one UGC research project on "Development of ES for control of 4 legged robot device model.". One UGC research project is ongoing under innovative scheme. At PG level also he has guided more than 300 projects/discretion. He has published more than 150 papers in International & National level Journals and also International Conferences and National level Conferences. He has also successfully completed the Software Development & Computerization of Finance, Library, Exam, Admission Process, and Revaluation Process of Amravati University. Also completed the Consultancy work for election data processing. He has also worked as member of Academic Council, selection Committee member of various Other University and parent university, Member of faculty of Engineering & Science, BOS (Comp. Sci.), Member of IT Committee, Member of Networking Committee, Member of UGC, AICTE, NAAC, BUTR, ASU, DRC, RRC, SEC, CAS, NSD etc committees. . He has also worked chairman of many committees like BOS, Monitoring and Control, New Installations, Curriculum design and developments etc. He has organized more than 50 Summer schools / STTP/ Conferences / Seminar /Symposia / Workshop /Orientation Program/Training/Program / Refresher Courses. He is member and fellow of Learned Societies like Institute of Engineers, Indian Society of Technical Education ISTE, Computer Society of India CSI, etc. He has delivered more than More than 70 Keynote addresses and Invited talks delivered in India and abroad at the occasion of International & National level Technical/social events, International Conferences and National level Conferences, and also acted as session chairs many times. 3 times he has received National Level excellent paper award at National Conference, Gwalior and at other places. He has also received UGC fellowship and a major UGC project. (e-mailid: vilthakare@yahoo.co.in)