International Research Journal of Engineering and Management Studies (IRJEMS)
Volume: 03 Issue: 05 | May -2019 ISSN: 2395-0126

COMPRESSED SENSING BASED INTRUSION DETECTION SYSTEM AND INTRUSION PREVENTION SYSTEM IN WIRELESS SENSOR NETWORK

K.Abinaya[1], V.Sathya[2],
PG Student, Department of CSE, A.V.C college of engineering, Mannampandal, India
abinayakarnan95@gmail.com
Assistant professor of CSE, A.V.C college of engineering, Mannampandal, India
saro.sath@gmail.com

Abstract - *In order to ensure the reliability and credibility of the data in wireless sensor networks (WSNs), this paper proposes a trust evaluation model and data fusion mechanism based on trust. First of all, it gives the model structure. Then, the calculation rules of trust are given. The trust evaluation model is comprehensive trust consists of three parts: behavior trust, data trust, and historical trust. Data trust is calculated by processing the sensor data's Based on the behaviors of node in sensing , forwarding. The behavior trust is obtained the initial value of historical trust is set to the maximum and updated with comprehensive trust in compressed data. Comprehensive trust can obtained by weighted calculations, and then the model is used to construct the trust list and guide the process of data fusion. Using the trust models to simulation results indicate that energy consumptions can be reduced by the average of 15%. The detection rate of abnormal nodes is at least 10% higher than that of the lightweight and dependable trust system (LDTS) model. The impact of the proposed trust model in data prediction and Compressed Sensing (CS) based aggregation and reconstruction is validated using various performance metrics and different attack models.*

Key Words: *compressed sensing, TAR, TSTM,IDS,IPS.*

1. INTRODUCTION

WSN are composed of many sensor nodes. These nodes are usually used to perform some specific monitoring tasks. They can obtain the monitoring data in an area, and the data are transmitted to the control center for further analysis. However, the open environment of the WSNs makes nodes easily exposed to a variety of attacks, such as eavesdropping, node compromising, and physical disruption. These attacks are likely to lead to unreliable data. Therefore, it is necessary to develop measures to ensure data reliability and reduce energy consumption. The motivation in this work is based on the idea that the trust value of an object can be reflected by the data and behavior of the object. For example, consider the case of an object that is abnormal. It will bring abnormal data or behavior. In fact, any application scenarios that involves data-aware and data forwarding can be supported by such a framework.

2. LITERATURE SURVEY

Anastasi G et.al., [1] Discuss about the wireless sensor networks (WSNs) have gained increasing attention from both the research community and actual users. The sensor node are generally battery-powered device in the network process, the critical aspects to face concern how to reduce the energy consumption of nodes, so that the network lifetime can be extended to reasonable times. The first break down the energy consumptions is the component of a typical sensor nodes, and discuss the main directions to energy conservation in WSNs.

Liu X et.al., [2] focus to the Data collection is a crucial operation in wireless sensor networks. The designs of the data collections an schemes is challenging due to provide limited energy supply and the hot spot problem. Leveraging empiricals observation that sensors data based possess strong spatiotemporal compressibility, this paper proposes a novel compressive data collection scheme for wireless sensor networks. adopt a power-law decaying datas model verified to the real data sets and then propose a random projection based estimation algorithm for this data model. Requires fewer compressed measurements, the greatly reduces the energy consumption. It allows simple routing strategy without much computation and control overheads, which leads to strong robustness in practical applications. Analytically, we prove that it achieves the optimal estimation error bound.

Wu M &Tan L [3] Discus about the Environmental monitoring is one of the most important applications of wireless sensor networks (WSNs), which usually requires a lifetime of several months, or even years, the inherent restrictions of energy carried with in the battery of sensor nodes bring an extreme difficulty to obtains a satisfactory network lifetime, which becomes a bottleneck in scale of such applications in WSNs.

Ngugen MT & Rahnavard N [4] Discuss about the compressive sensing (CS) and clustering in wireless sensor networks (WSNs) is proposed to significantly reduce the energy consumption related to data collection in such networks. The compressive sensing (CS) and clustering have been proved to be efficients ways of reduced the energy consumption in WSNs, however, there is little study about the integration of them for further gains. The idea is to partition a WSN into clusters, in which each cluster head collects the sensor readings within its cluster and forms CS measurements to be forwarded to the base station.

Yu Y et.al.,[5] Focus to the trust issue in wireless sensor networks is emerging as one important factor in security schemes, it is necessary to analyze how to resist attacks with a trust scheme. It is categorized various of types of attack and countermeasures related to the trust schemes in WSNs. then provided to the level of development in prosess the development of trust mechanisms, give to a short summarization of classical trust methodologies and emphasize the challenges of trust scheme in WSNs.

3. SYSTEM DESIGN

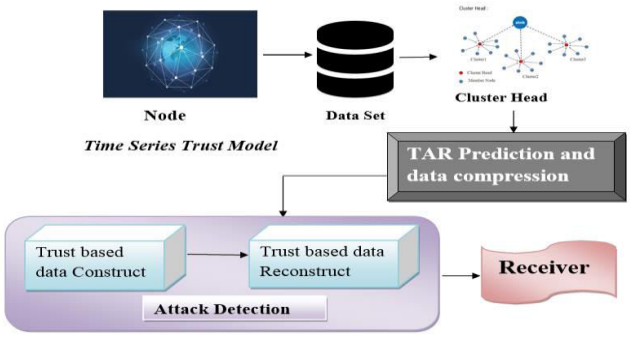


Fig -1: System architecture

To enhance the utilization of wireless resources, clustering as a method of user cooperation is often considered in the conventional wisdom. In wireless environments, antenna deployments, the proximity of users, and scattering around users can cause correlative signal transmission paths between user device, and thus high correlations between channels may occur when user devices are dense. Under these circumstances, the similarity with respect to channel state information (CSI) among different user devices can be exploited to enable channel cluster formation. With each formed cluster, messages from the base station are directly sent to cluster members by multicast, which can enhance resource utilization.

4 .MODULES

The modules of the proposed system are follows

- Time series trust model
- TAR Prediction and data compression
- Construct and Reconstruct
- Attack detection

4.2.1 Time series trust model

TSTM has been proposed based on data trust, energy trust and relative trust in every node in the network. It is assumed that the WSN is homogenous and all nodes have the same communication range and initial energy level. However, the CHs are assumed to be more robust with more energy than the other nodes. These nodes are clustered using k-means algorithm. At a particular time instant t , the Total Individual Trust (TIT) of a node is calculated based on energy trust (ENtrust) and data trust (DAtrust). Energy of a node is a very vital metric and it is defined as a function of distance of the node from the cluster head . Abnormal amount of energy is consumed, when a node is under attack. Since malicious nodes consume more energy while selfish nodes require remarkably lesser energy, the value of ENtrust in the proposed model ensures that the requirement of data accuracy, integrity and authentication is met. The data trust is defined as in and the relative trust is modelled.

4.2.2 TAR Prediction and data compression

Secure data prediction based on linear and non-linear autoregressive (AR) model with the trust model as

exogenous input (TAR) in the Cluster Heads head (CH). CS based data compression in the CHs. Time-series data of temperature and humidity have been used to develop linear and non-linear AR based prediction models. The trust value based on TSTM has been used as exogenous input for the AR model. The CHs uses the TAR model to predict the data. They also compress the data received from the nodes in their respective clusters based on the compression ratio. The CHs transmit the compressed data to the base station. The base station reconstructs the original data based on the trust value modelled by TSTM.

4.2.3 Construct and Reconstruct

The CHs uses the TAR model to predict the data. They also compress the data received from the nodes in their respective clusters based on the compression ratio. The CHs transmit the compressed data to the base station. The base station reconstructs the original data based on the trust value modelled by TSTM. The development of Auto Regressive models with eXternal input (ARX) as time-series trust value is a major contribution of this work. The linear and nonlinear (ARX models) and their modeling techniques are described in the next section.

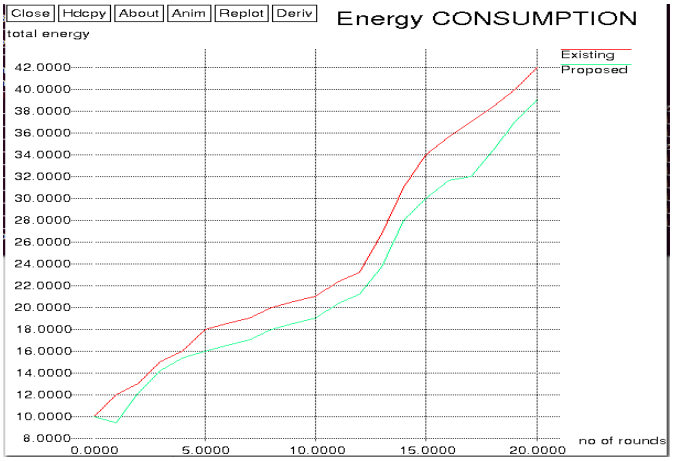
4.2.4 Attack detection

Attack matric used to recognizing attacks. To reconstruct the complete metric data and detection. Calculates attack matric data with compressive sampling. The attack matric data are encapsulated into independent detection packets and sent to the network. Time-series data of temperature and humidity have been used to develop linear and non-linear AR based prediction models. The trust value based on TSTM has been used as exogenous input for the AR model. The CHs uses the TAR model to predict the data. They also compress the data received from the nodes in their respective clusters based on the compression ratio.

5. RESULTS AND DISCUSSIONS

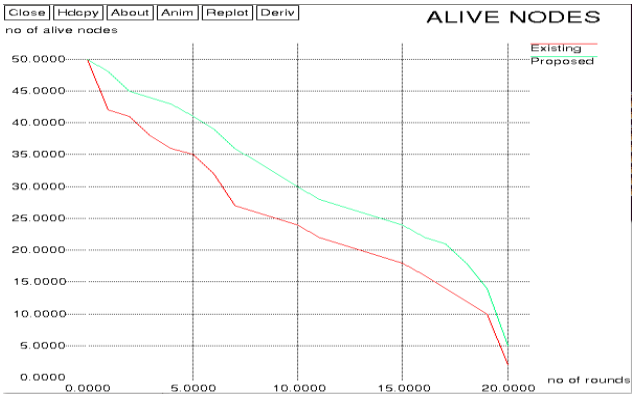
The performance of the CS-based data aggregation, compression and reconstruction has been evaluated at a particular time instant for two different compression ratios with different number of clusters. The compression ratio is defined at the ratio between numbers of nodes to the number of measurements. The robustness of the proposed trust model is validated by testing its performance during the occurrence of three different kinds of attacks.

ENERGYCONSUMPTION:



The attack model 1 is Sybil attack which is a node replication attack. This attack takes place when the attacker creates large number of pseudonymous identities by node replication. The attack model 2 is bad mouthing attack in which the attackers give a negative feedback about the victim. The attack model 3 is the data forgery attack and this attack includes data addition, deletion and modification.

PACKET DELAY:



The performance of both TSTM and EDTM is quite similar for Sybil and badmouthing attacks but TSTM performs slightly better for data forgery attack. The performance of trust-based data reconstruction at the base station during malicious node attack has been evaluated. The accuracy of reconstruction of data from a particular cluster for which Node 10 was the CH was tested with varying percentage of malicious nodes and the results.

6. CONCLUSIONS

The novel trust evaluation methodology for data prediction, aggregation and reconstruction has been proposed for compressed sensing based clustered WSN. A Time Series Trust Model (TSTM) at the node level has been proposed and the time series trust value is used as exogenous input to Trust based Auto Regressive (TAR) model for data prediction at the cluster head. The TAR model is built using linear and nonlinear algorithms namely wave net and tree partition. The proposed models were tested for three different attacks. The TAR model built on tree partition performed better than the Efficient Distributed Trust Model. Compared with the evaluation model (which only focuses on the behaviour trust), our model has a higher abnormal detection rate. In addition, the trust value is calculated by a simple weighted average method. Therefore, it is light enough to fit well with WSNs without great overheads. The performance of trust based reconstruction was also tested and the trust based Basis Pursuit algorithm performed better than the least squares algorithm. In order to validate the proposed models, communication overhead analysis of the TSTM and power consumption analysis of the prediction and aggregation algorithms were performed.

7.2 FUTURE ENHANCEMENTS

Application of the proposed methodology in heterogeneous large scale networks is the future direction of this research work. The performance of these models for other applications will also be tested in the future. The efficiency of the proposed models in multi-hop routing both in inter-cluster and intra-cluster scenario is also an area to be explored in the near future. The proposed scheme can be extended by integrating the state of the art schemes such as full duplex, energy harvesting, cognitive radio networks and vehicular ad hoc networks.

REFERENCES

[1] Anastasi, G., Conti, M., Di Francesco, M., & Passarella, A. (2009). Energy conservation in wireless sensor networks: A survey. *Ad hoc networks*, *7*(3), 537-568.

[2] Liu, X. Y., Zhu, Y., Kong, L., Liu, C., Gu, Y., Vasilakos, A. V., & Wu, M. Y. (2015). CDC: Compressive data collection for wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, *26*(8), 2188-2197.

[3] Wu, M., Tan, L., & Xiong, N. (2016). Data prediction, compression, and recovery in clustered wireless sensor networks for environmental monitoring applications. *Information Sciences*, *329*, 800-818.

[4] Nguyen, M. T., & Rahnavard, N. (2013, November). Cluster-based energy-efficient data collection in wireless sensor networks utilizing compressive sensing. In *MILCOM 2013-2013 IEEE Military Communications Conference* (pp. 1708-1713). IEEE.

[5] Yu, Y., Li, K., Zhou, W., & Li, P. (2012). Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures. *Journal of Network and computer Applications*, *35*(3), 867-880.

[6] Zhao, J., Liu, H., Li, Z., & Li, W. (2012, October). Periodic data prediction algorithm in wireless sensor networks. In *China Conference on Wireless Sensor Networks* (pp. 695-701). Springer, Berlin, Heidelberg.

[7] Jellali, Z., Atallah, L. N., & Cherif, S. (2016, September). Linear prediction for data compression and recovery enhancement in wireless sensors networks. In *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)* (pp. 779-783). IEEE.

[8] Wang, W., Wang, D., & Jiang, Y. (2017). Energy efficient distributed compressed data gathering for sensor networks. *Ad Hoc Networks*, *58*, 112-117.

[9] Jiang, J., Han, G., Wang, F., Shu, L., & Guizani, M. (2015). An efficient distributed trust model for wireless sensor networks. *IEEE transactions on parallel and distributed systems*, *26*(5), 1228-1237.

[10] Chen, Z., Hartmann, A., & Goldscheider, N. (2017). A new approach to evaluate spatiotemporal dynamics of controlling parameters in distributed environmental models. *Environmental modelling & software*, *87*, 1-16.