Intrusion Detection Based on State Context and Hierarchical Trust in Wireless Sensor Networks

Mrs.M.Swarna Sudha
Assistant Professor(SG)
Computer Science and Engineering
Ramco Institute of Technology
Rajapalayam

Harini Subramanian, Lavanya Sankari N, Mahalakshmi S
Computer Science and Engineering
Ramco Institute of Technology
Rajapalayam

ABSTRACT

Security problems have become obstacles in the practical application of wireless sensor networks (WSNs), and intrusion detection is the second line of defense. In this paper, an intrusion detection based on dynamic state context and hierarchical trust in WSNs is proposed, which is flexible and suitable for constantly changing WSNs characterized by changes in the perceptual environment, transitions of states of nodes, and variations in trust value. A multidimensional two-tier hierarchical trust mechanism in the level of sensor nodes (SNs) and cluster heads (CHs) considering interactive trust, honesty trust, and content trust is put forward, which combines direct evaluation and feedback-based evaluation in the fixed hop range. This means that the trust of SNs is evaluated by CHs, and the trust of CHs is evaluated by neighbor CHs and BS; in this way, the complexity of evaluation is reduced without evaluations by all other CHs in networks. Meanwhile, the intrusion detection mechanism based on a self-adaptive dynamic trust threshold is described, which improves the flexibility and applicability and is suitable for cluster-based WSNs.

KEYWORDS

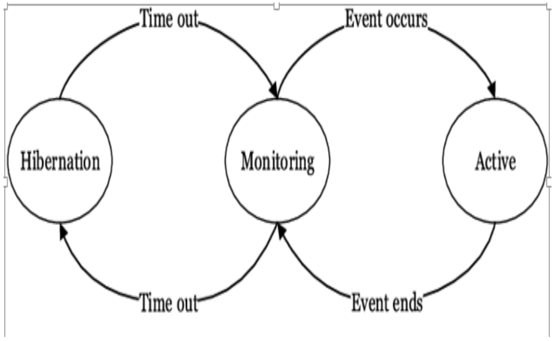
Hierarchical trust, trust evaluation, state context, intrusion detection, wireless sensor network.

I. INTRODUCTION

Sensor networks have recently emerged as a platform for several important surveillance and control applications.Sensor nodes are typically less mobile, more limited in capabilities, and more densely deployed than mobile ad-hoc networks (MANETs). This necessitates devising novel energyefficient solutions to some of the conventional wireless networking problems, such as medium access control, routing, self-organization, bandwidth allocation, and security. Exploiting the tradeoffs among energy, accuracy, and latency, and using hierarchical (tiered) architectures are important techniques for prolonging the network lifetime. Wireless sensor networks (WSNs) are widespread in a variety of areas, including environmental monitoring, battlefield observation field,and the nodes in WSNs should cooperate with each other for communication and support of high-level application.

The main contributions of our work are as follows:

1) **State context construction** : By analyzing the states of nodes in WSNs, a state transition context and its judgment rules are established, through which different methods could be adopted to calculate trust value effectively, i.e. a selfadaptive trust calculation method for SNs. Meanwhile, the details of the possible security problem according to the state conversions are analyzed.
2) **Hierarchical trust improvement** : Two-tier hierarchical trust mechanism is proposed, which refers to the trust of SNs and the trust of CHs. The judgment strength of the SNs' trust is reduced by CH-to-SN trust evaluation, whereas the judgment strength of the CHs' trust is enhanced through CH-to-CH, the feedback of 1-hop neighbors of CHs and BS-to-CH trust evaluation. The mechanism is suitable for clustered WSNs with multidimensional observing data.



3) **Detection threshold self-adaption:** malicious detection process, the threshold of detection could be adjusted according to the operation of WSNs rather than a fixed value, which improves the self-adaption and detection rate of the system
4) **Resource conservation considerations:** Sensor nodes, measures should be taken to reduce resource consumption, including ten-scale integer representation of trust value, spatial correlation and alleviation of the computing tasks of SNs through CHs and BSs responsible for more computational tasks.

II. RELATED WORKS

The research on trust mechanisms in WSNs and other networks is widespread, e.g., Underwater Acoustic Sensor Networks (UASNs), Medical Sensor Networks (MSNs) and Vehicular Networks (VNets) these approaches are often used to assess data integrity, secure routing, message authenticity, reliability and the security of nodes. ng, message authenticity, reliability and the security of nodes. Trust-based intrusion detection is a typical application of reliability and security of nodes.

However, the node with the maximum number of interactions with neighbors was considered as the most trustworthy in the process of the calculation of the intimacy trust inspired by social networks. The difference in our work is the consideration of the reasonable range of the maximum number of interactions, as interaction that exceeds the range indicates malicious behavior. A new function of interactive trust evaluation is put forward in our work.

A series of theoretical proofs were given in the research to verify the effectiveness of the mechanism. In the process of trust evaluation, only successful and unsuccessful interactions were taken into consideration, with no other trust evaluation factors taken into account. The mechanism in our work takes interactive trust, honesty trust and content trust into account, addressing problems of consuming energy maliciously and tampering multidimensional observing data with lower resource overhead, which is described in the performance evaluation.

We consider a clustered WSN consisting of multiple clusters, each with a cluster head (CH) and a number of SNs in the corresponding geographical area with CHs having more computational and energy resources than SNs. A SN forwards its sensor reading to its CH and the CH then forwards the data to the base station or a destination node (or sink node) through other CHs Our trust-based IDS scheme considers the effect of both social trust and QoS trust on trustworthiness or maliciousness. In the literature, social trust may include friendship, honesty, privacy, similarity, betweeness centrality, and social ties (strengths). QoS trust may include competence, protocol conformance, reliability, task completion capability, etc. In this work, we adopt honesty to measure social trust derived from social networks and adopt energy (for measuring competence) and cooperativeness to measure QoS trust derived from communication networks, as these can be considered as indicators of trustworthiness. The honesty trust component is measured through evidences of dishonesty such as false self reporting trust fluctuation and abnormal trust recommendations (i.e., outliers relative to recommendations received from other recommenders).

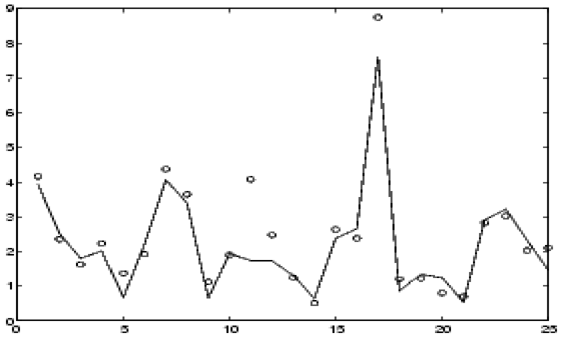
The mechanisms they presented consume more storage of nodes and CHs because they have to store the trust value of all other nodes, including both the direct trust value and indirect trust value or the recommended trust. The overhead of our method (trust evaluation and intrusion detection) is concentrated on CHs and BSs with much greater resources than SNs, which will prolong the lifetime of WSNs.

Dhakne and Chatur proposed a distributed trust-based intrusion detection approach in WSNs, which considered multidimensional trust on energy, data and communications, evaluating direct trust, recommendation trust and indirect trust of nodes, and detected malicious nodes through the deviation of subjective trust and objective trust. The ability of detection is improved by multidimensional trust, whereas the data trust in DTBID refers to 1-dimensional data, and multidimensional data are not discussed in DTBID. It is essential to take multidimensional observing data into account because it is common for several kinds of sensors to be carried on a node to observe different data. The content trust in our approach could evaluate multidimensional observing data to discover data tampering attacks.

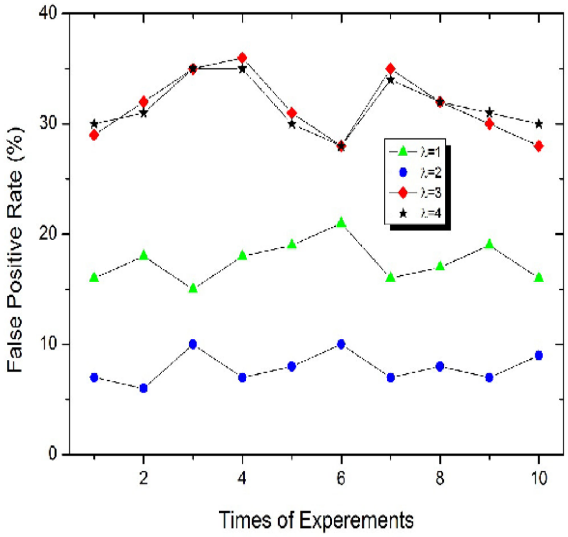
The system adopts Dempster-Shafer theory to improve the detection rate, and it could be used in the network of fixed nodes and mobile nodes. It is designed for detecting sinkhole attacks, and other attacks would escape from detecting. Our approach is suitable for hybrid attacks including tampering, black hole, selective forwarding and other energy consumption attacks due to multidimensional trust evaluation.

III. SYSTEM MODEL

We consider a clustered WSN consisting of multiple clusters, each with a cluster head (CH) and a number of SNs in the corresponding geographical area with CHs having more computational and energy resources than SNs.



Data transmission features of common WSNs used for monitoring are introduced; then, the spatial correlation of nodes is described for energy preservation. Our trust-based IDS scheme considers the effect of both social trust and QoS trust on trustworthiness or maliciousness.



In the literature, social trust may include friendship, honesty, privacy, similarity, betweeness centrality, and social ties (strengths). QoS trust may include competence, protocol conformance, reliability, task completion capability, etc.

IV. METHODOLOGY

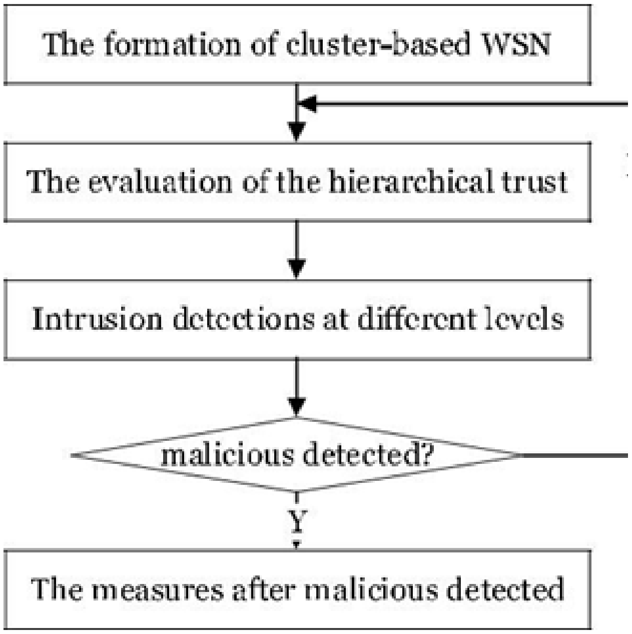
Clustering algorithm for comparison,

- **Fuzzy c-means**-It is a method of clustering which allows one piece of data to belong to two (or) more cluster.It is frequently used in pattern recognition.It is also known as Fuzzy ISODATA.FCM is an iterative algorithm.The aim of FCM is to find clusters centers that minimize a disimilarity function.This algorithm is useful when the required number of cluster are pre-determined.This tries to put each of the data prints to one of the clusters.FCM is different in that it does not decide the absolute membership of a data point to a given cluster instead it calculates the likelihood that a data point will belong to the cluster.The major advantages are unsupervised and always converges.The cons of this method is long computational time,sensitivity to the initial guess (speed,local minima), and sensitivity to noise.

- **Subtractive clustering method**-One pass algorithm for estimating the number of clusters and the cluster centers in a set of data. It is a fast, one-pass algorithm for estimating the number of clusters and cluster centers in a set of data.The cluster estimates obtained from the sub clusters function can be used to initialize iterative optimization-based clustering method (FCM) and model identification methods. The subclust function finds the clusters by using the subtractive clustering method.

- **Semantic-driven subtractive clustering method**–It is used in advancement of SCM and it uses axiomatic fuzzy sets. Aiming at the unnecessary need of manual input of parameters t1 and t2,we propose a semantic driven clustering method((SDSCM) to improve the traditional subtractive clustering algorithms by introducing the axiomatic fuzzy sets(AFS)theory. The density radius t1 is a automatically determined and weight r2 is semi-automatically determined based on the membership matrix.We compare the SDSCM with the KMEANS on the iris and wine datasets. Experimental results show that the SDSCM is one percentage to 5 percentage higher that the FCM and the KMEANS in terms of evaluation index (semantic strength expectation),while the SPT is lower than the two methods,where it still needs to be improved.The SDSCM can effectively solve the disadvantages caused by manual input of parameters t1 and t2, and find the cluster which are closer to the user semantics.

V. FLOW OF DESIGN


The formation of cluster-based WSN
The evaluation of the hierarchical trust
Intrusion detections at different levels
malicious detected?
Y
The measures after malicious detected

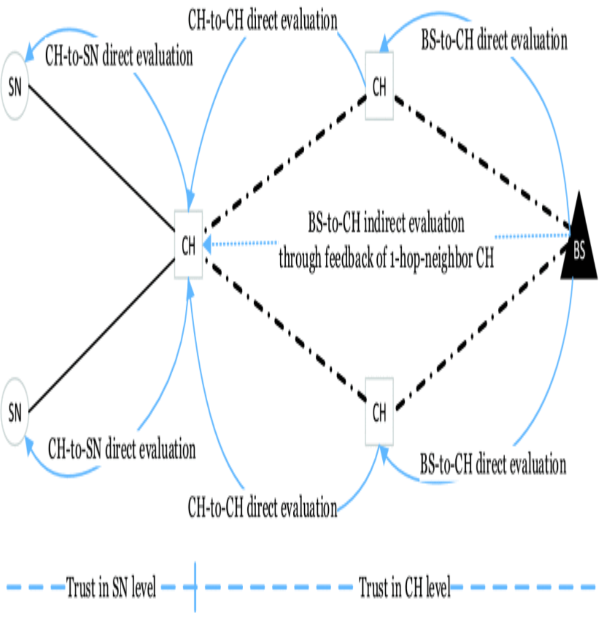
VI.NETWORK MODEL AND ASSUMPTIONS

States and transitions

Sensor nodes in WSNs are in different states to conserve energy,and it is not necessary for all nodes to appear to be active all the time due to the restriction of resources.The state of nodes are considered including hibernation,monitoring and active,which are the basic and necessary state and other state are not taken into consideration here. The transitions of different states depend on predefined rules, such as timeout or event occurrences. If monitoring node discovers an event, it will be revert to an active state to deliver more information about the event. When the events end, the state o the node returns to monitoring. Normal transitions and attacks could be distinguished by trust calculation. Hence, state transition is the context of trust calculation, and data transmission rate is the context of state transition.

VII.AN IMPROVED HIERARCHICAL TRUST MECHANISM

In this section, an improved two-tire hierarchical trust mechanism is introduced, which consist of SN trust evaluation and CH trust evaluation.Based on the cluster-based WSN described in, a two-tier hierarchical trust mechanism is introduced.Unlike prior works,the first level trust is simplified by CH-to-SN evaluation due to the direct communication between SN and CH in a cluster,whereas the second level trust is conducted by CH-to-CH direct evaluation and BS-to-CH direct or indirect evaluation through the feedback of a one-hop-neighbor CH.


CH-to-CH direct evaluation
CH-to-SN direct evaluation
BS-to-CH direct evaluation
SN
CH
CH
BS-to-CH indirect evaluation
through feedback of 1-hop-neighbor CH
BS
SN
CH
CH-to-SN direct evaluation
BS-to-CH direct evaluation
CH-to-CH direct evaluation
Trust in SN level
Trust in CH level

This is shown in which we can see that the evaluation of trust is expected by CHs and BSs. The evaluation of the trust is periodic, the update cycle of which Del t, a predefined interval according to the operation of WSN.

VIII.REFERENCES

[1]I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, ‘‘A survey on sensor networks,’’ IEEE Commun. Mag., vol. 40, no. 8, pp. 102–114, Aug. 2002.

[2] I. Onat and A. Miri, ‘‘an intrusion detection system for wireless sensor networks,’’ in Proc. IEEE Int. Conf. Wireless Mobile Compute. Netw. Commun, Aug. 2005, pp. 253–259.

[3] The UK Commission for Employment and Skills. *The Labour Market Story: Skills For the Future*, 1st ed.; The UK Commission for Employment and Skills (UKCES): London, UK, 2014

[4] Handel, M. Trends in Job Skill Demands in OECD Countries. OECD Social, Employment andMigration Working Papers, No. 143, 2012. Available online: http://dx.doi.org/10.1787/5k8zk8pcq6td-en (accessed on 18 October 2015).

[5] Y. Yu, K. Li, W. Zhou, and P. Li, ‘‘Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures,’’ J. Netw. Compute. Appl., vol. 35, no. 3, pp. 867–880, May 2012.

[6] O. Khalid et al., ‘‘Comparative study of trust and reputation systems for wireless sensor networks,’’ Secur. Commun. Netw. vol. 6, no. 6, pp. 669–688, 2013.