International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

Network Database Security in Wireless Sensor Networks with Intellectual Access of using Outlier Detection Techniques

K.Satya Rajesh, N.RaghavendraSai, Ch.Nagamani

ABSTRACT---In the field of information mining, exceptions are likewise alluded to as outliers, variations from the norm, discordant perceptions, or freaks. Other application spaces may utilize terms like exceptions, amazements, or contaminants. Every one of these wordings is catching a deviation from an expected ordinary information demonstration. In this research work, another system that comprises of an Intelligent Agent Based Access Control subsystem and Intrusion Detection subsystem for securing the Web Database has been proposed and actualized. With a specific end goal to give a viable access control framework, new access control variable based math and new arrangements utilizing rules have been proposed and executed. Keeping in mind the end goal to perform interruption and outlier identification successfully, a half and half Intelligent Agent based Intrusion Detection framework has been proposed in this work which enhances the security of the network database.

Keywords: Wireless sensor networks, Intrusion Detection System

I. INTRODUCTION

Wireless sensor networks (WSN) were develop for a broad range of social and military applications, such as production line, object tracking, infrastructure monitoring, habitat sensing, and frontline surveillance [1], [2]. One basic feature of WSN function is to gather information in between the source station and the target location(s) where the target phenomena were observed. Aforementioned feature usually desire multi-hop packet transmission if the distance from the source to the target phenomena is large. For example, a cluster-based sensor network [3], [4] necessitates a different source of information must travelled single-recipient communication paradigm via multi-hop packet transmission (shown in Figure 1). Further, to decrease communication interference in highly dense wireless networks, the communication range of radios must be decreased. This results in multi-hop transmission as well.

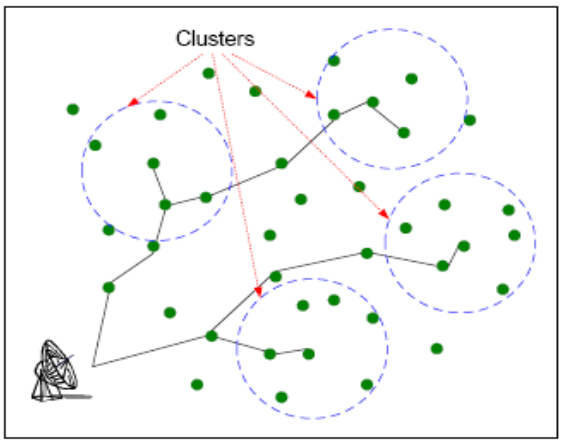

Fig. 1. Multi-hop packet transmission in a sensor network

One suitable methodology for reducing the radio power consumption is the so-called modulation scaling [5], which discovers the tradeoff between transmission energy and time duration by that condition, the modulation level to equal the different traffic load. An important examination is that in many coding schemes, suppose w(t) is the energy used for transmitting a packet over units (t) of time, w(t) is a non-negative, monotonically decreasing, and strictly convex function of (t) [6].

Therefore, the challenge is to identify patterns in data that do not align with the behavior predicted. Outlier detection is commonly used in various applications, for example credit card fraud detection, insurance and healthcare, cyber safety intrusion detection, defense critical systems malfunctioning and enemy military surveillance. Outer identification is important because outliers in data often mean interesting (and often critical) actionable information in a wide variety of fields of operation.

II OUTLIER LOCATION IDENTIFICATION METHODS

In numerous data processing tasks, a large amount of data is being collected and processed. One prime step in procurement a coherent analysis is the detection of anomalous observations. Outlier detection refers to the problem that trends are observed in data are not consistent with the normal expected behaviour. Outlier detection involves the process of identifying data objects that do not

Revised Manuscript Received on December 30, 2019.
* Correspondence Author
K.Satya Rajesh, HOD, Dept. of Computer Science, C.S.T.S Govt, Kalasala, Janagreddygudem, W.G. Dist, A.P, India. (Email: ksatyarajeshcse@gmail.com)
N.RaghavendraSai, Assoc. Prof, Dept. of CS &Engg, KoneruLakshmaiah Education Foundation, Vaddeswaram, AP, India.
Ch.Nagamani, Research Scholar, Department of Computer Science, AcharyaNagarjuna University, Guntur, A.P, India.

compromise with the remaining objects in the data set. Such irregular patterns also involve outliers, deviations, exceptions, discordant findings, faults, aberrations, failures, sounds, accidents and errors as well as surprises, novelties, toxins, etc. In spite of the terms noise or error, these are also considered to carry important information.

For a number of applications, additional detection procedures have been proposed, such as credit card fraud detection, clinical trials, irregularity analysis of the voting system, data cleaning, weather intrusion, geographic information systems, sport performance analyzes and other datamining assignments.Detecting outliers is of utmost importance as they might lead to model misspecification, biased parameter estimation and improper results. This process of detecting outliers should be done prior to analysis and modeling.

III. NETWORK OUTLIER DETECTION SYSTEM ALGORITHM

The proposed Network outlier detection system(NODS) algorithm will effectively identifies the anomalies in the network database system and enhances the security of the network database.

- x is the initial record from dataset.
- R is the Record set.
- K is the distance from one node in network to other node.
- A is the cluster set created from K with all records
- Identify() function is used for detecting outliers in the network with R Records.

Function NODS()
Let $\{ x_i \in R^d, i=1,\ldots,N \}$ be the data vectors in the training set;
Calculate the distance $K(x_i,x_i)$ to origin for each data vector x_i;
Obtain
$A=\{K(x_i, xi), i=1,\ldots,N\}$;
return R = Identify (A, 1, n, $[v_n]$+1)
Function Identify (list, l, r, n)
if
l=r
return list [l]
anomaly = l + floor (rand () * (r−l+1))
anomaly = Outlier(list, $l, r,$ anomaly)
if n = anomaly
return list [n]
else if $n <$ anomaly
return Identify(list, $l,$ anomaly − 1, n)
else
return Identify (list, anomaly + 1, r, n)

In the proposed method, Let R is the Data vectors considered in the trained data set. Distance K is calculated between hubs in the network. Identify() function is called which is used for detecting outlier IDs in the considered network. Outlier() function considers for the highlighting of identified outliers from the network so as to take necessary action on the network for secure data transmission. The identify() is called in any one of the three cases i.e, if all anomalies are identified, then the list will be returned. If specified anomalies are not identified, then again identify() is called otherwise other anomalies are identified till all records are monitored.

IV RESULTS

The productivity of the proposed Network Based Outlier Detection calculation is likewise contrasted with Nested Looping calculation utilizing the informational indexes. The new proposed calculations are nearly tried utilizing different informational collections. The execution of the above said calculations are pictorially represented.

It likewise demonstrates the different execution time of the above said calculation against the quantity of information focuses. The execution time is appeared in seconds. This diagram is drawn by taking the quantity of information focuses in X-hub and the execution time in Y-pivot.

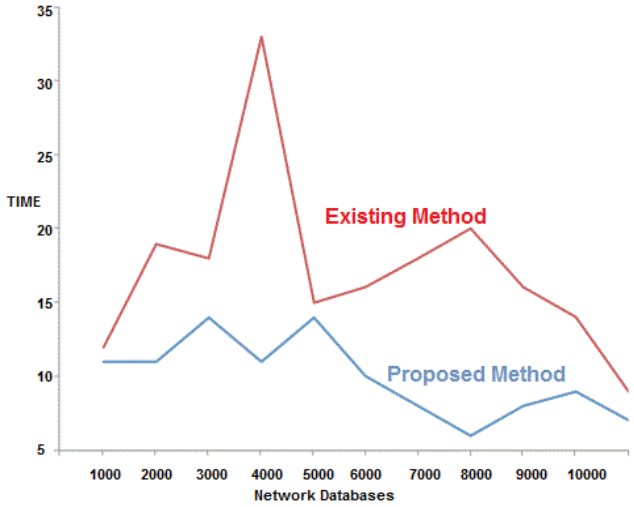

Fig 5.1 Comparison of Execution Time amongst proposed and existing calculations

The outlier detection rate analysis based on node longitude location value and the degree of the node is illustrated in the below graph.

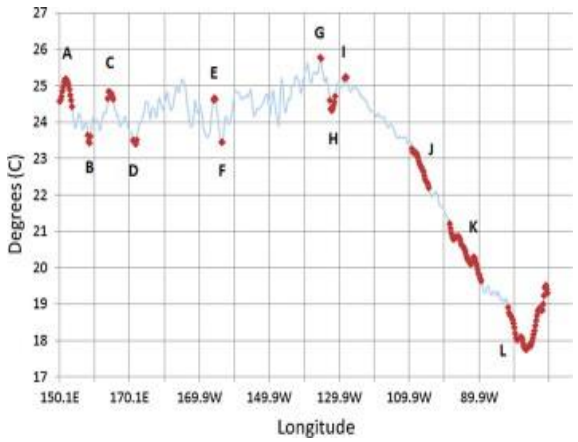

Fig 5.2 Outlier Detection Rate

V CONCLUSION

The proposed framework introduced a two-level half and half interruption location technique in light of directed and anomaly strategies. This technique shows extraordinary execution in perceiving remarkable characterization ambushes and likewise tremendous scale attacks new and presented strikes when attempted with a NSL KDD datasets. In furthermore considers, this system will attempt to influence a more suitable social affair to approach in light of speedier and profitable classifiers with a specific end goal to make a basic duty in the examination of the outlier acknowledgment. In this research work, another system that comprises of an Intelligent Agent Based Access Control subsystem and Intrusion Detection subsystem for securing the Web Database has been proposed and actualized. With a specific end goal to give a viable access control framework, new access control variable based math and new arrangements utilizing rules have been proposed and executed. Keeping in mind the end goal to perform interruption and outlier identification successfully, a half and half Intelligent Agent based Intrusion Detection framework has been proposed in this work which enhances the security of the network database.

REFERENCES

1 D. Estrin, L. Girod, G. Pottie, and M. Srivastava, “Instrumenting the world with wireless sensor networks,” in *The International Conference on Acoustics, Speech and Signal Processing*, May 2001.
2 G. J. Pottie and W. J. Kaiser, “Wireless integrated network sensors,” *Comunications of the ACM*, vol. 43, no. 5, pp. 551–558, May 2000.
3 M. Singh and V. K. Prasanna, “A hierarchical model for distributed collaborative computation in wirelss sensor networks,” to appear on 5th Workshop on Advances in Parallel and Distributed Computational Models.
4 Y. Yu, B. Krishnamachari, and V. K. Prasanna, “Cluster-based lightweight middleware for a class of wireless sensor networks,” submitted to IEEE Network Magazine.
5 C. Schurgers, O. Aberhorne, and M. Srivastava, “Modulation scaling for energy-aware communication systems,” in *ISLPED*, 2001, pp. 96–99.
6 B. Prabhakar, E. Uysal-Biyikoglu, and A. E. Gamal, “Energy-efficient transmission over a wireless link via lazy packet scheduling,” in *INFOCOM*,
7 2001.
8 W. Ye, J. Heidemann, and D. Estrin, “An energy-efficient MAC protocol for wireless sensor networks,” in *Proc. of INFOCOM*. New York, June 2002, pp. 1567–1576.

AUTHORS PROFILE

1. *Dr K. Satya Rajesh* received Ph.D Degree from Rayalaseema University, Kurnool. He received Master’s degree M.C.A from ManonmaniamSundarnar University in 2003. He received Master’s degree M.Tech in Computer Science & Engineering from AcharyaNagarjuna University in 2010. He is currently acting as a Head of the Department of Computer Science in C.S.T.S Govt. Kalasala, Jangareddygudem, W.G Dist A.P., India. His research interests are Computer Networks & Sensor Networks. He had published several papers in National and International Conferences & International Journals. He is a member of IACSIT, IAENG and also review member of many Journals.

N.RaghavendraSai, Assoc. Prof, Dept. of CS &Engg, KoneruLakshmaiah Education Foundation, Vaddeswaram, AP, India. His interested areas are Data warehousing and Data mining, Computer Networks.

Ch.Nagamani, Research Scholar, Department of Computer Science, AcharyaNagarjuna University, Guntur, A.P, India.Pursing Ph.D. from Nagarajuna University. Here interested areas are Data warehousing and Data mining, Data Analaytics Computer Networks.