ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105

International Journal on Recent Researches In Science, Engineering & Technology

(Division of Computer Science and Engineering)

A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. It is an absolutely free (No processing charges, No publishing charges etc) Journal Indexed in JIR, DIIF and SJIF.

Research Paper

Available online at: www.jrrset.com

Volume 5, Issue 1, January 2017.

JIR IF : 2.54
DIIF IF : 1.46
SJIF IF : 1.329

Data Anticipation and Synthesis Pattern in Wireless Sensor Network for Hub Appliance Based Computerized Substantial Structure

R.Kiruthika[1], K.Rajeswari[2]

[1,2]Assistant Professor, Department of Computer Science and Engineering, Mahendra Engineering College, Mahendhirapuri, Namakkal District, Mallasamudram, Tamilnadu, India.

Abstract:

Wireless Sensor Network (WSN) is a sensor-associated data another system security circumstance shrewd examination forecast technique is proposed, which applies GM (1,1) model and back propagation neural system display in the systematic expectation field of system security circumstance data, and mix and enhancement is performed to it to enhance the exactness of system security circumstance expectation. By breaking down and computing the immense measure of data gained from arrange security circumstance assessment framework, it can make expectation on the present security circumstance of system framework and its future change pattern. This system executes relative reaction technique as indicated by forecast comes about, and lessen the mischief from organize assaults and enhance the crisis reaction capacity of system data framework. The proposed system Forecast-based Protected Information Intelligence (FPII) improves the forecast precision and assurance the communication secrecy using Grey Model (GM) with the goal that can make readiness before extraordinary harm happens and decrease or stay away from any conceivable assault to guarantee the smooth running of framework.

Keywords: Forecasting information, Gray model, Encoding, Data set, WSN.

Introduction

Wireless Sensor Networks (WSNs) have gained worldwide attention in recent years. These sensors are small, with limited processing and computing resources and they are inexpensive compared to traditional sensors. In modern wireless communication security and privacy have become an increasingly indispensable part. Wireless sensor nodes in the network are deployed in order to transmit sensitive information such as financial data, health monitoring, civilian and military application, thermal, biological, chemical, optical and magnetic sensors may be attached to the sensor node to measure properties of the environment.

Smart sensor nodes are low power devices equipped with one or more sensors, a processor, memory, a power supply and a radio. A variety of mechanical since the sensor nodes have limited memory and are typically deployed in difficult-to-access locations, a radio is implemented for wireless communication to transfer the data to a base station. Battery is the main power source in a sensor node. Secondary power supply that harvests power from the environment such as solar panels may be added to the node depending on the appropriateness of the environment where the sensor will be deployed.

Related Work:

Wireless Sensor Networks (WSNs) are widely used in agricultural, environmental, industrial, and military monitoring applications. WSNs consist of many minute sensor nodes, which collect data from their surrounding environment and send it to a base station. The sensor nodes themselves are rather limited in resources but communicate with each other and with the base station using short-range wireless communication.

Energy based AODV (E-AODV) [1] that assures the security of privacy, Integrity and Availability triangle. Privacy is provided by computing Intermediate Trust Value (ITV) for all nodes between source and destination. The highest ITV nodes are used for data transmission. The digital signature algorithm provides data integrity. Availability has been provided by computing the residual energy of every node so that nodes that possess the highest energy are used for data transmission. A Reliable Route Selection Scheme (RRSS) [2] estimates the node's arrival angle using RSS variations to obtain route's lifetime and to decision about the convenience of an adjacent node. However, this method does not detect the unreliable node in the network. Game theoretic approach [3] detects the malicious node and improves the network throughput. Distributed detection scheme detects the malicious node rapidly, and that a mobile malicious node can only avoid detection for a very limited time period [4]. Random seed distribution [5] assumes the random allocation of secret material and a transitory master key that is used to create a pair-wise key. Key agreement protocol [6] was used in communication and true relay participation in the public exchange. The tradeoff between security and protocol efficiency is measured in the join design of advantage refinement, privacy amplification, and information resolution. This method achieves positive secret key rate while an opponent has more favorable channel conditions. Hop-by-Hop Authentication Scheme (HHAS) [7] was based on Elliptical Curve Cryptography (ECC) that provides mediate node authentication and source privacy. This scheme reduces the computational and communication overhead.

Angular Routing Protocol (ARP) based on a position that uses an improved geographic forwarding to route packets to the destination. The geographic forwarding fails, at a time used by the angle-based forwarding method. It does not require establishing routes [8]. The indefinite node estimates its angle to each of the three reference nodes, based on these angles, and the positions of the reference nodes and computes its own position using simple trigonometrical relationships [9]. Orthomorphic Analyst-Nearest Neighbor method detects the intrusion activity based on the traffic intensity at inner boundary instance within the communication MANETs. Angle based distance is measured between the node points for easy detection of traffic creating nodes. It measures how far each pair of mobile nodes is and evaluates correct angle of position within the inner boundary[10]. The angle is found based on a slope of the line. Slope values are found in all neighboring nodes. The angles between the unidentified node and several fixed nodes are used in the AOA (angle of arrival) to evaluate the position, which is a little costly to perform [11].

Forecast-based Protected Information Intelligence (FPII) – Proposed Model

In this FPII scheme, the architecture for the WSN that enables algorithm design and synthesis is designed. Architecture represents the abstract machine model for designing algorithm. Synthesis and a set of primitives that are self-determining of protocols used to transmits the data from one hub to other hub in the network. The simulation analysis is used for monitoring the behavior on a sensor network.

Topology Formation:

In wireless networks, a topology is a generally conventional description of the organization of a network, consist of sensor nodes. There are two methods of defining network such as physical signal topology. The physical topology is geometric layout of workstations. Signal topology denoted by nature of the paths from hub to hub.

Primitives represent the transformation of designing an algorithm into a program for the make the network. Programming primitives: The virtual architecture specifies the computation and communication primitives available to the programmer. These primitives could be for the individual node or for a set of nodes (collective). Data transmission primitives are send() and receive() message passing primitives for group communication. Computation primitives could include summing, sorting, or ranking a set of data values from a set of sensor nodes.

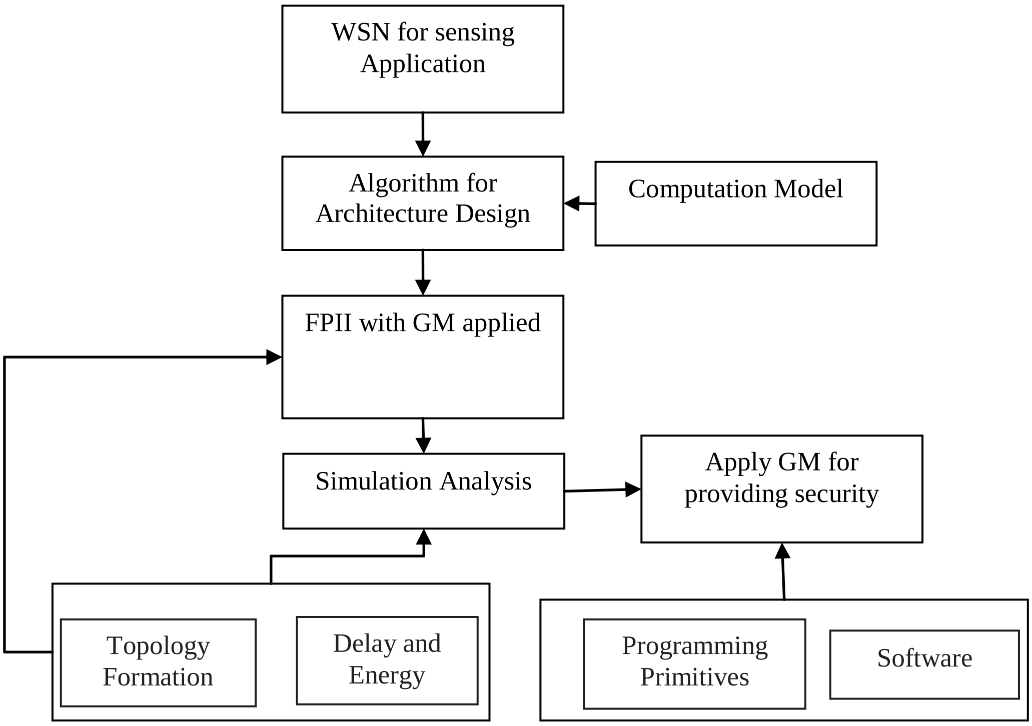

Fig.1 Architecture of Proposed Scheme

Gray Model – Forecast Method

Grey Model represents a system which has incomplete information about it and makes the system uncertain. Only a a small number of data can be used in GM for estimation of unknown system [12]. To exemplify the system behaviour it is featured by a first order differential equation. Due to restricted storage limitations cannot be able to provide whole and absolute information entire WSN. It in this way can be dealt with as a dim framework with questionable or deficient data during the time spent information detecting and combination.

Both the sink hub and sensor hub direct expectation utilizing similar information succession and forecast instrument. With the underlying anticipated information arrangement of size n, another information succession of size (n + 1) can be gotten by means of GM(1,1). The sensor node obtains the forecasted data with help of GM (1,1) then the next set of obtained data x(x+i) is modified by calculating the error e(i+1). After encoding the obtained data (x+i), the sensor node sends the encrypted data to the sink hub.

On the off chance that the blunder between them is under the edge ε, it is superfluous for the sensor hub to send the information to sink hub, and the vitality is spared, while accomplishing the objective of information combination. In the mean time, the sink hub likewise utilizes a similar forecast instrument to anticipate the information of next period and after that considers the anticipated information as the detected information in current period. Moreover, the sensor hub ought to transmit the detected information to sink hub using GM for encoding when the forecast mistake is past the edge ε. It ought to be called attention to that ε is characterized by end-clients and it can be balanced. At that point the forecast precision will be impacted with distinctive estimations of ε which is considered as threshold.

Simulation Analysis

Evaluation of the proposed protocols achieved using simulations in the network simulator. Such simulations use the common parameters indicated in Table 1. Performance evaluation of the proposed protocols is provided by estimating the Packet Delivery Rate, Packet Loss Rate, in the network.

Table 1: Simulation Parameters of FPII

Parameter	Value
Channel Type	Wireless Channel
Radio Propagation model	TwoRayGround
MAC type	802.11
Simulation Time	100 s
Number of nodes	50
Transmission range	250m
Traffic model	CBR
Simulation Area	1000x1000

The simulation is done by using the simulator NS2. Network simulator is a discrete event time driven simulator. NS2 is open source software which uses C++ and Tool Command Language (TCL) for simulation. C++ is used for packet processing and fast to run.

Packet Delivery Rate:

Packet delivery Rate is defined as the ratio of total data packets received by the destination to total send packets by source multiplied with a number of receivers. The PDR is calculated by the equation (6).

$$PDR = \frac{Total\ Pack\ Received}{Total\ Pack\ Send} \qquad (6)$$

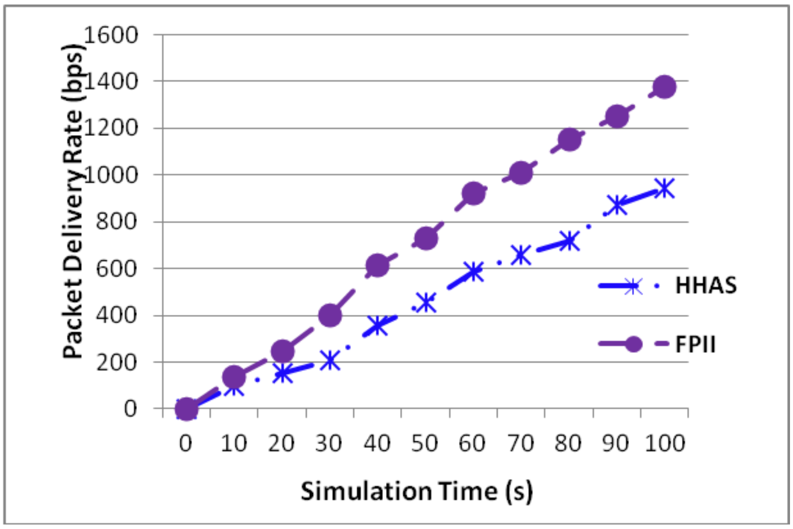

Figure.2 Packet Delivery Rate

From figure 2, the proposed protocol FPII that increases the packet delivery rate compared to the existing protocol HHSA. In FPII, transmit the data through the reliable routing path as a result increase the PDR but HHSA decreases PDR because of it transmits the data through the adversary path.

Packet Loss Ratio (PLR):

The Packet Loss Rate (PLR) is the ratio of the number of packets dropped to the number of data packets sent. The PLR is calculated by Equation (7).

$$PLR = \frac{Total\ Pack\ Dropped}{Total\ Pack\ Send} \tag{7}$$

The figure 3 indicates the packet loss rate of the proposed protocol is lesser than the HHSA protocol showing the efficiency of the FPII.

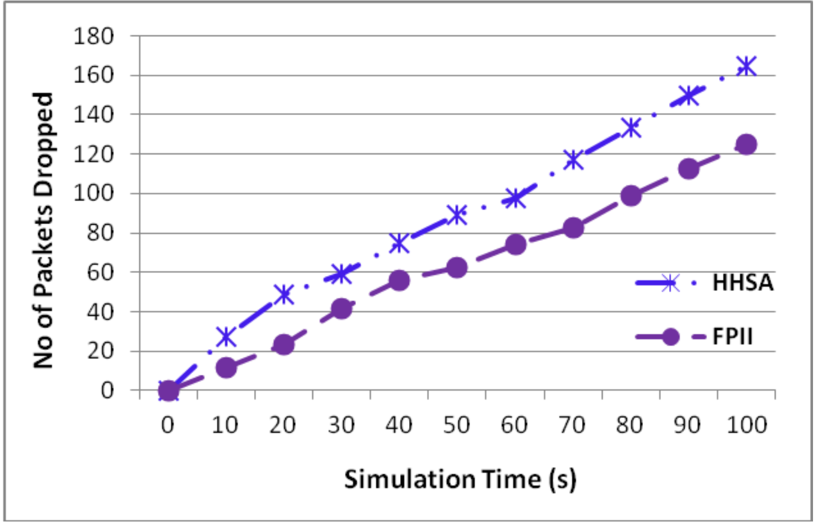

Figure.3 Packet Loss Rate

Conclusion

WSN is a sensor-associated data in which forecast technique is proposed which applies GM (1,1) model to enhance the exactness of system security circumstance expectation. By breaking down and computing the immense measure of data gained from arrange security circumstance assessment framework, it can make expectation on the present security circumstance of system framework and its future change pattern. This system executes relative reaction technique as indicated by forecast comes about, and lessen the mischief from organize assaults and enhance the crisis reaction capacity of system data framework. The proposed system FPII improves the forecast precision and assurance the communication secrecy by verifying the threshold with the goal that can make readiness before extraordinary harm happens.

References:

1. Sumathi A, Sundaram VB. An ANN Approach in Ensuring CIA Triangle using Energy based Secured Protocol E-AODV for Enhancing the Performance in MANETS. Indian Journal of Science and Technology. 2015; 8(34).
2. Reina DG, Tora SL, Jonhson P, Barrero F. A Reliable Route Selection Scheme Based on Caution Zone and Nodes' Arrival Angle IEEE Communications Letters, 2011; 15(11).
3. Wang W, Chatterjee M, Kwiat K, Li Q. A game theoretic approach to detect and co-exist with malicious nodes in wireless networks. Computer Networks, 2014; 71:63-83.
4. Jun-Won H, Matthew W, Das SK. Distributed detection of mobile malicious node attacks in wireless sensor networks. Ad Hoc Networks 10. 2012; 512–523.
5. Gandino F, Montrucchio B, Rebaudengo M. Key management for static wireless sensor networks with node adding. IEEE Transactions on Industrial Informatics, 2014; 10(2):1133-1143.
6. Wang N, Zhang N, Gulliver TA. Cooperative key agreement for wireless networking: Key rates and practical protocol design. IEEE Transactions on Information Forensics and Security. 2014; 9(2):272-284.
7. Ian L, Yun L, Ren J, Wu J, Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks. IEEE Transactions on Parallel and Distributed Systems. May 2014; 25(5).
8. C. Venkata and M. Singhal, "Angular routing protocol for mobile ad-hoc networks," in proceedings of the 25th IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW '05), Columbus, Ohio, USA, June 2005.

9. A.Boukerche,H.A.B.F.Oliveira,E.F.Nakamura,and A.A.F. Loureiro, “Localization systems for wireless sensor networks,” IEEE Wireless Communications, vol.14,no.6,pp. 6–12,2007.
10. R. M. Chamundeeswari and P. Sumathi, “Efficient detection of intrusion using inner and outer boundary models with transductive learning concept in mobile Adhoc network,”Inter-national Journal of Scientific & Engineering Research, vol.5,no. 6, 2014.
11. L.Cheng, C.Wu,Y.Zhang,H.Wu, M.Li,and C.Maple, “A survey of localization in wireless sensor network,”International Journal of Distributed Sensor Networks,vol.2012,ArticleID 962523, 12 pages, 2012.
12. F.M. Tseng, H.C. Yu, G.H. Tzeng, Applied hybrid grey model to forecast seasonal time series, Technol. Forecast. Soc. Change 67 (2001) 291–302.