pp.173:180

Intrusion Detection in Wireless Sensor Networks using Genetic Algorithm

Elham Yazdankhah[1],Fardad Farokhi[2], Reza Sabbaghi-Nadooshan[3]

[1,2,3]Electrical Engineering Department,Tehran University of Central, Tehran, Iran. Email: Elham_yazdankhah@ymail.com, f_farokhi@iauctb.ac.ir, r_sabbaghi@iauctb.ac.ir

Abstract
Wireless sensor networks, due to the characteristics of sensors such as wireless communication channels, the lack of infrastructure and targeted threats, are very vulnerable to the various attacks. Routing attacks on the networks, where a malicious node from sending data to the base station is perceived. In this article, a method that can be used to transfer the data securely to prevent attacks is suggested. The selection based on optimal path by routing using genetic algorithm uses. The proposed optimal paths to transmit data perceived to have chosen and ensures reliable data transmission.

Keywords: genetic algorithms, wireless sensor networks, malicious nodes, intrusion detection.

1. Introduction

A wireless sensor network (WSN) consists of sensor nodes that may be scattered in a vast area. Tiny sensor nodes with limited computation and communication capabilities are fed by the battery. These tiny sensor nodes are capable to different types of attacks. For a large-scale wireless sensor network, monitoring and protection from physical attacks are not practical for each individual sensor. Attacks in wireless sensor networks can be classified on the physical layer, communication (media access control or interface), network, transport and application layer. The attacks can also be divided into two categories: internal and external. An external attacker does not have access to most encryption components in a sensor network, while an internal attacker may have access to some of the key components and is trusted by some of the other nodes. It is very difficult to identify and deal with internal attacks [1].

Wireless sensor networks for sensing environmental events and transmit information to the base station is used for processing. Thus, routing in sensor networks is an important operation. The best way of security to detect routing attacks in these networks is routing [2].

Classical intrusion detection mechanism in sensor networks due to scarcity battery and processing resources are limited enforcement capabilities. Therefore, an effective scheme to detect malicious attacks, a powerful and effective approach is needed. Sensors, energy, bandwidth, storage and processing capability are limited. They used widely station security, target identification, exploration, medical applications, etc. Measures are necessary to detect an attack aim at destabilizing the network is to be implemented. Thus, the need for secure communications to prevent data interception, analysis, and modification by an intruder there is vital. Intrusion detection systems, security breaches patterns in a system with monitoring and trend analysis detects activity.

Genetic algorithm is similar to the immune system. The abnormalities are determined and are removed by measuring deviations from normal processes and by using a distributed IDS system with the recognized and adapted relationship. This algorithm is inspired by some of the natural

mechanisms that include: production, mutation, selection and composition. Selected solutions for optimization problems, role play element and function costs of these components and people decide which solutions are remained. Evolution of population with applying the above mentioned cases continues to reach a good solution (not the best) [3]. In this research genetic algorithms for wireless sensor network intrusion detection used. So survey previous algorithms, this algorithm comes to the conclusion that the genetic algorithm for intrusion detection is the best solution. In the rest of the paper, Section 2 is background. Section 3 proposes the algorithm,and Section 4 shows the results. Finally, Section 5 concludes the paper.

2. Background

Genetic algorithm, proposed by Charles Darwin in 1858, is a random search techniques mimicry natural evolution. Successful combination of genetic algorithm is applied to a whole range of problems. They are useful especially in applications design and optimization of the number the variables are too complicated algorithms or procedures [13].

The genetic algorithm is based on the principle of natural selection, in which each possible solution as a binary string (chromosome) and measure relevant are displayed graceful, steady solutions as part of an evolutionary process in which one individual solution are selected from the other set increases for the next generation is made. Individuals with high fitness as likely to choose the strategy of the parent population are selected with the assumption that they have a better solution in the next generation (subsequent run) are produced. Fitness solutions with much weaker normally be set aside. There are also a small chance of some weaker solutions may remain in the selection process as is possible genes involved in this process may be mainly composed of the intersection, will be useful. Mathematically, the probability of selecting a potential solution is proposed:

$$P_i = \frac{F_i}{\sum_{j=0}^{N} F_j} \quad (1)$$

Where P_i is the probability that a particular solution is selected for the parent population. Fi represents the fitness function and N is the total number of potential solutions in a crowd. Genetic algorithm has proven to cases in which the search space is large, complex and not well understood and there is almost no domain knowledge can be useful. They can arbitrary large number of variables, constraints and objectives to manage multiple [13][14].

Optimized sensor networks [6], using genetic algorithm each sensor node is assigned a function. These functions are described as: 1- disable node (off), 2- cluster head (CH), 3- router between cluster (ICR) and 4 - sensor node (NS). Each cluster is managed by the cluster heads and cluster members by the sensor nodes and ICR are shown. Cluster head can perform combining data from different sensor nodes. While the router (ICR) between clusters, cluster data to the base station directs. Sensor networks, a multi-objective genetic algorithm (MOGA) is defined by the competitive fitness functions, genetic algorithm to optimize the assignment of critical mass battery, choosing the optimal path, optimal positioning using a proper security features are implemented.

3. The proposed algorithm

In the proposed model, the base station as a trusted component that is intended to send a secure relationship between different types of nodes leads to secure data. Nearest nodes to the base station make sure the highest regard to base station. Nodes further away from the security hierarchy, which is the beginning of a base station, which is a predetermined routing decisions during start up and during reconfiguration have been created, is apparent. The security architecture can be sent of the constituent elements of the relationship between different types of nodes related reasons run the command / message data, etc. Any authentication is done via a base station components and the hierarchical routing. After detection, the re-node clustering adverse event is triggered when the node is open to doing different objectives to create an energy-efficient sensor networks: 1) re-join the cluster, 2) re-dynamic routing and 3) re-assigned security features sensor.

Genetic algorithm-based approach IDS, including LMN Prksy range that will monitor and communicate is again any deviations from standard specifications established during initialization or configuration. LMN optimal number and positioning of monitoring with minimum overhead cover provides maximum power. Productivity can be achieved by avoiding the assignment of monitoring nodes to monitor the track, cluster or Routers that are below the threshold increased confidence. Confidence threshold is created by monitoring traffic monitoring and feedback nodes as a function of the size of propriety. LMN function only can be used by cluster head and or routers in the cluster considered. From a

security standpoint, each node can be used as a standard node or a node monitor using a chromosome screen revealed. Chromosome genetic algorithm includes all the building blocks of a solution of the problem at hand, is located that is suitable for genetic operators and fitness function. Also it is called 'strands'. Each CH or ICR is shown binary digits called a gene. A Bit of gene allele defines the attributes of a node is called a: 0: No special treatment of node (NOP), 1: local monitoring node: is defined, monitoring the base station. Each string is set of functional characteristics as explained above, of each CH or ICR. Fitness function called 'measures trusts' for each field to be examined. Greater proportion is of delegates representing optimal performance due to suspicious activity, desired coverage and battery power remaining in the system are evaluated [12].

3.1. Local monitoring node (LMN)

Local monitoring node to the base station is a trusted proxy agent. Base station offers LMN to act as a CH or ICR. In the case of CH, could be any one of its members as the choice of nodes to use for the purpose of monitoring, which can node to increase cluster heads are selected from the search scope. After selecting the cluster head as LMN, the base station receives the signal strength information (RSS) is a member of the nodes to be able to listen to supervised cluster (Suspicious). This information are used CH to select one of its members as a representative to monitor the cluster through or under the ICR. LMN chromosome sequence in Fig. 1 is shown with 10001, in which LMN function has been assigned the nodes. 1(CH-1) and 6(ICR).Base station is sent specific patterns through loop-bake recipe LMN (CH-1) using route 4 → 5 → 1 → P → B . Reply to message be returned route B → 2 → 6 → 5 → 4. The proxy chosen by p CH-1 (LMN) 5 blocks to monitor cluster nodes 2 (oval spot by dot) [12].

Due to the broadcast nature of communication sensor node, the target node LMN are assessing continue to monitor the items that are said to be. (a) receives signal strength, (b) transition, (c) fraudulent transfer nodes that are not neighbors, (d) delay the response or lack of response to the test patterns, and (e) waste packages or changes. For example, in Fig. 1, the proxy LMN (P) can be monitored (listen), the data are addressed from node B to node 2 or elsewhere. In addition, the base station makes use as an agent back for the transfer of specific patterns through the path of trust and receive patterned using a pre-established route.

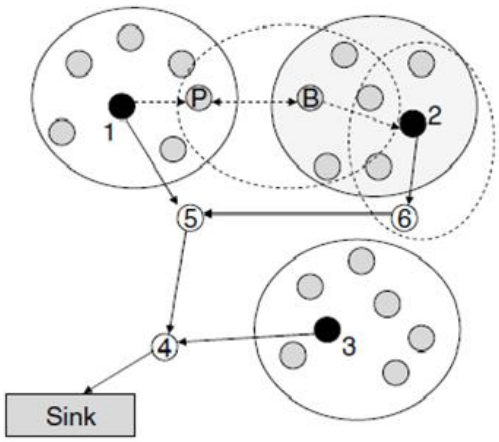

Fig.1. Local control mode to CH-1 (node 1) and ICR6 (node 6) 2 has been assigned to cover the suspected cluster. Both LMN, the cluster offers 2 full coverage.

Here are the steps on each node is considered a model extracted from the data and then unique sensor ID in the general level (GUID) and using key Contact nodes (INCK) hash and it adds to packet delay. Hash data as a pre-established pattern, the next step in the path is used [5]. Packet delay in specific patterns by the LMN monitor will revert to the base station. This process is repeated through all the steps to the base station, the data are used to identify malicious nodes or setting out its authenticity (IR). LMN in the vicinity, who are all neighboring nodes to monitor, the whole WSN base station for monitoring anomalies. Base station uses LMN warnings with traffic data analysis and ranking clusters based on the integration path deviation from the standard specification. These structures are identified of Clustering behavior or pathways in terms of statistical metrics and models of observed activity. Statistical models used by the base station may be an operational model, the mean and standard deviation of models, multivariate models, Markov process models, time series models, and etc. [10][11].

3.2. Fitness function

Optimality criteria fitness function to monitor the position of the nodes (for example, LMN) is a sensor network and the identification of clusters or routers misplaced. The fitness function fit with other criteria relevance such as batteries fit, the load balancing is competing [4] [5]. As a dynamic process that occurs over the lifetime of the system. Different elements of fitness function are as follows:

3-2-1 Fitness function properly monitored nodes (MIF)

This component of the fitness function is to oversee the allocation of cluster or a path that is suspected of being compromised. Base station to check each unique path through the cluster and may be based on the messages that it supervises, and 10,000 scale them based on a set of rules to rank. This value is called the right place and a low value indicates a high influence is suspected.

$$MIF = \frac{\sum_{ch=1}^{N} IR_{CH}.k_{CH}}{\sum_{ch=1}^{N} K_{ch}} + \frac{\sum_{icr=1}^{M} IR_{icr}.K_{icr}}{\sum_{icr=1}^{M} K_{icr}} \quad (2)$$

$$K_x = 1, if\ x = LMN; X \in (ch, icr) \quad (3)$$

$$IR_{icr} = \frac{\sum_{r=1}^{R} IR_{icr}^{r}}{R} \quad (4)$$

Here IR_{ch} and IR_{icr} sequence CH and ICR are correct rank order. R is the number of paths, and IR^{r}_{icr} the right way rank r routh, which consists of ICR as a routing path. IR base station is evaluated with an assessment of past traffic patterns, to estimate the location of the current LMN recorded using correlation, analysis of covariance (Eq. (5)) between data packets x and y, in violation of the parameters of quality of service (QoS)(e.g., delay guarantee, improper formation package) and reporting of adverse power conditions with respect to the base station based on the expected traffic load [12]. An essential aspect of the history is used for the selected amount of time. A short history may be inadequate to observe the process, while longer history can affect trends based on the distant past. For traffic patterns, exponential smoothing model (Eq. (6)) to predict the characteristics of the packet arrival process and the distribution of counts (IDC) (equation (7)) to check for tandem use a particular route.

$$R_{x,y} = \frac{cov(x,y)}{var(x).var(y)}; \quad -1 < R_{x,y} < 1 \quad (5)$$

$$\bar{\lambda}(t) = \alpha.\lambda(t-1) + (1-\alpha).\bar{\lambda}(t-1) \quad (6)$$

$$IDC = var(\sum_{k=0}^{n} \lambda_k)/E(\sum_{k=0}^{n} \lambda_k) \quad (7)$$

Where λ (t) is the actual number of packet arrivals in the interval t, ، $\bar{\lambda}(t)$ is the estimated number of packet arrivals in the interval t, and λ_k is of the packet arrival intervals τ_k and τ_{k+1}. It is a measure of the fluctuation rate received over a given distance. The correct size based on feedback from current LMN or if the node is involved in more suspicious routes, decrease finds [12].

3-2-2 Fitness function node battery status (MBF)

Whenever a sensor node to the cluster head or a cluster with routers communicate between clusters, a penalty to be paid for using batteries. During battery operation, and other relevant functions are used observation. Each node to the base station battery status (Q), and use of batteries periodically (synchronization node) or the quantum limit (or threshold) passes, warns. These thresholds can be used for sentences using this node to monitor operations consume more battery power. The penalty for the node with a low battery capacity and residual capacity depends on the type of node. Fit the battery condition is expressed as follows:

$$MBF = \frac{\sum_{i}^{N} BC_i.K_i}{\sum_{i}^{N} K_i}; \qquad BC_i = f(Q,U) \quad (8)$$

Where Q is the remaining battery capacity, BC_i predicted battery capacity of node i (CH or ICR) between 0 and 1. Battery usage rate (U) depends on the individual load on each node and can be estimated by observing traffic patterns and data synchronization nodes. According to the evaluation of genetic algorithm, LMN is changed dynamically position themselves to maximize the efficiency of energy distribution so that the sensor network is uniformly used [12].

3.2.3. Monitoring node coverage value Fitness (MCF)

Monitoring node coverage value LMN, that can cover the maximum number of nodes with a rank just below their quest to find the attacker. Table base station for each cluster in the right place and route (base station) holds. The end result is to maximize the proportion of coverage desired coverage suspected malicious as well as non-suspicious nodes. However, to maximize coverage for malicious node tries nondestructive nodes if convergence is possible, but the rewards are included to cover more malicious nodes.

$$MCF = \frac{1}{2}\left(\frac{\beta_1.\sum_{i}^{N}\psi_i}{F_1.N} + \frac{\beta_2.\sum_{j}^{M}\psi_j}{F_2.M}\right) \quad (9)$$

$$\beta_1 + \beta_2 = 1; \quad (10)$$

Where ψ_i total operating LMN that the node is malicious i monitor that is less than the threshold level is correct, ψ_j number of factors LMN that the node non-destructive j monitors above the threshold level and F1 , F2 respectively redundancy of coverage for each node is malicious and non-malicious. Redundancy can cover up the base station to check the sensor positioning using multiple techniques to help. Coverage decisions based on the information RSS available at the base station in the initialize or re-clustering phase is placed last. During each of these stages neighbors CH data RSS from the base station transmits its members [12].

3.2.4. Proportion of cumulative trust Fitness (CTF)

Fitness associated with local monitoring node is local in a fit of cumulative trust (CTF) is specified.

$$CTF = \alpha_1 MIF + \alpha_2 MBF + \alpha_3 MCF \qquad (11)$$

Where $\alpha_1 + \alpha_2 + \alpha_3 = 1$, MIF fitness function properly monitor node, MBF fitness function node battery status, MCF monitoring coverage of the node, weight each component depends of on the implementation and the relative importance. These values can be used to adapt foreign exploration [12].

4. Results and Discussion

Classical intrusion detection mechanism in sensor networks due to scarce battery and processing resources are limited enforcement capabilities. Therefore, an effective scheme to detect malicious attacks, a powerful and effective approach is needed. Sensors have limited energy, bandwidth, storage and processing capabilities. Measures are necessary to detect an attack aimed at destabilizing the network is to be implemented. When all nodes are placed in listen mode, genetic algorithm with crossover 60% and initial mutation 6% runs. Using Matlab software for monitoring the status of node and security features have been implemented. The fit parameters is calculated (section 2.3), depending on traffic patterns, the integrity of packages downloaded using the battery, and monitoring coverage. These data fit the parameters of the genetic algorithm estimates. While objective genetic algorithm tends to converge to the equilibrium system, the end result lives up to networks for optimal coverage. Furthermore, malicious nodes introduce with similar characteristics but transmission limitation and some different attack messages.

For the detection and recognition of malicious nodes based on varying number of malicious nodes focus. In Fig. 2, the proportion of malicious nodes, the nodes non-destructive between 0.05 and 0.25. The results obtained are compared with respect to detection LMNs. At the same time destroying all nodes are placed in random positions. Recognition continues until all malicious nodes are detected. Fig. 2, the average detection time increases with the proportion of malicious nodes in the show. LMNs at the time of detection averaged 50-60% decrease. Detection time, additional improvement with a large number of malicious nodes shows, because even if the packet traffic monitoring nodes increase the efficiency of the detection process and the characteristics of the feedback process is simple. Even if LMN extra energy to detect the profile to use, faster detection of malicious nodes also means for the rest of the nodes are longer battery life. To optimize battery performance due to LMN, monitoring frequency based on the neighboring nodes monitor a variety of characteristics, that are adapting.

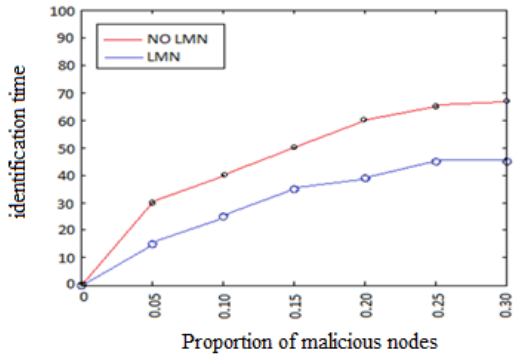

Fig.2. Average time to identify all nodes compromised as a function of the number of malicious nodes.

Fig.3 shows positive detection rate as a function of the number of malicious nodes. Positive rate due to misdetection as a legitimate node happens to be a bothersome. This can disrupt the integrity of the system and the efficiency of routing and clustering algorithms to reduce, because observation and analysis of data can be compromised malicious node undesirable clustering and decision optimization will trigger [6][7]. Rather than run as long as malicious nodes are detected, the detection of stationary state to be kept. LMN positive rates is compared range from 2.5 to 5 percent by 9-15% classic mode (no LMN). Similarly, detection faster, reliability, increased energy costs and improve the network lifetime in the presence of compromised nodes increases. Improved the detection of false triggers as a result of incorrect data analysis due to nodes that are indistinguishable

from the base station does not have any knowledge of it lessens, reduces.

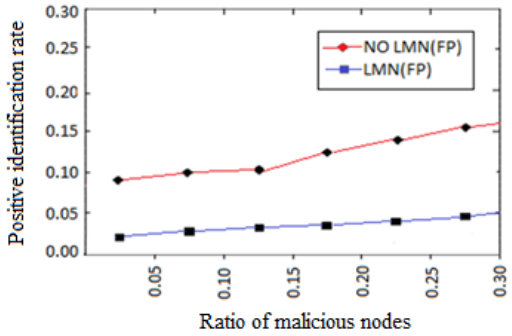

Fig.3. The positive rate of detection as a function of the relative number of malicious nodes.

To provide Quality of Service (including power consumption, bandwidth, etc.) sensor networks secure routing protocol multiple are provided. Design an efficient routing protocol, quality of service is one of the most important challenges in this type of networks. Routing protocols can be classified according to type: based-query, based-discussion, based-Quality of Service. Sensor network attack is an attacker, according to different purposes, energy in the sensor nodes are reduced and whereas that energy consumption impact on during network lifetime, network lifetime is reduced. A secure routing without regard to the amount of stored energy should not be used repeatedly to transmit packets of energy for all the nodes on a path to be a cavity in the network's connections creates. So energy is considered as a major challenge in ensuring quality of service in wireless sensor networks. Hence many protocols have tried to improve the reducing power consumption. The algorithm proposed in this paper is based QOS using genetic algorithm. As Kim and Cho [16] have provided based on a genetic algorithm, a method of producing a reliable way to transfer data to address areas that have been hit, have provided. In this paper an optimal route said based on genetic algorithms for secure transmission of data to the base station. Proposed fed, the base station selects the best route in terms of energy consumption. Which energy consumption is an improvement over successive generations, and the optimal way to avoid attacks on the network provides. So can taking a balanced energy depletion of the sensor nodes and the whole network, to guarantee the secure transmission of data. In addition, the genetic algorithm to find an efficient way, taking the attack, and the energy consumption needed for data transmission uses. The Al-Ghazal et al [17] and Guo et al. [18] have shown that genetic algorithm to solve the problem of finding an optimal path for WSN works well. This algorithm on a group of optimal or suboptimal solutions during the search and the search of optimal path will result in a short time.

Fig.4 shows Genetic Algorithm and protocols THVR for network lifetime. THVR [8] is a protocol for packet forwarding rate, which has been recognized as a quality suitable for delivery retardation closed. However, the two-step protocol for routing information from neighboring uses. The main goal of this protocol is to reduce the DMR package. The wireless sensor networks are used straightaway. This protocol is a geographic routing, and each node is aware situation and your destination via GPS [9]. Data are exchanged among neighbors, neighbors is notified two-step and two-step and one-step. It used to work with two message transmission HELLO done. First, each node's data, such as ID, location, remaining energy and etc., to its neighbors will notice the next HELLO message each node with a neighbor, the neighbor sends its single step. Mobile networks have HELLO packets are sent periodically to the neighbors aware and able maintain to two-step data [8]. Genetic algorithm as discussed in the research for data transmission THVR protocol uses a two-step neighborhood information. However, genetic algorithm has less overhead THVR protocol. Overhead for collection and information dissemination network is dominant, the number of packets sent or received at different nodes to the base station is done in steps. For a node in the attack, packets sent in this area is doubled packets received, this means that most of the malicious nodes in the region have been attacked. And nodes outside the area to get rid of duration at around the base station send packets to the neighbor. The number of packets sent to neighbor nodes is more; less network information flow is restricted by an intruder identification. This can be done was abandoned routes. So there is a tradeoff between the overhead communication and accurately identify an intruder. In Fig. 4, the simulation has been tested for more than 100 nodes, show that the lifetime of sensor network with a genetic algorithm in comparison THVR protocol has been increased. Sensor network which has been attacked by malicious nodes, network nodes to send data to the base station than normal when the network is going to use more energy. Designed with genetic algorithm show that the nodes consume less energy than THVR, and therefore increases the network lifetime.

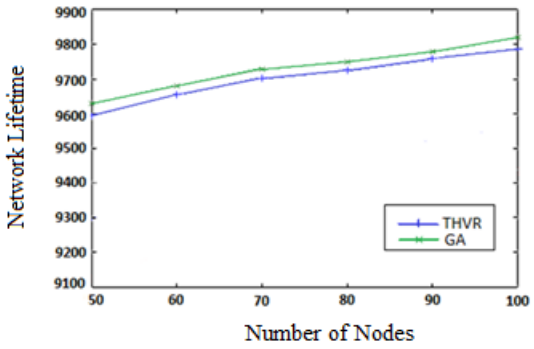

Fig.4.Comparison of lifetime of sensor networks using genetic algorithms with algorithms THVR.

To demonstrate the energy efficiency are used of a simple bit of arithmetic techniques. Fig. 5, Example of a linked list of bits in the message indicates.

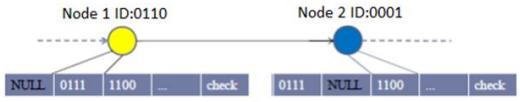

Fig.5. List of the bit attached to the message routing

Message routing is a 4-bit list, that are used to find the next node ID and control bits. Message Routing is the number of nodes on the path. First and last indexes of binding list in the first instance of message is control bit and NULL respectively. If NULL is in the first bit of the message, it is sent from the base station. When a node receives a routing message to the first instance is calculated by the XOR operation, first path bits in the list submitted to the next node determines its own. The attached list is updated in the message. If the node is a shift in the next position in the list is NULL. For example, if n is a node in the path, then the list is n+2. Node i receives the first message with the XOR operation with i +1 is calculated from the list of values. As shown in Fig. 5. Identity ID Node 1 and 2 are respectively 0110 and 0001. Node 1, the first node in the message path, routing can be transmitted to the next node ID using the index to find the NULL entries. 0001 via the XOR operation between 0110 and the second factor 0111 caused. Node information may be sent to the destination node using the XOR operation. According to data bits received by the destination node receives the routing message will be delivered in the reverse operation [15].

While reducing the power consumption of wireless sensor networks is one of the basic needs, supporting real-time communication network design seems more than ever. In fact, due to communication and interaction with the physical environment in real-time communication is essential in these networks, while significant challenges for real-time communication in wireless sensor networks, mainly due to restrictions that must be met simultaneously or according to the different applications of these restrictions will be removed at an acceptable level. For example, in many applications aimed at increasing the network lifetime and data delivery sensed from the environment, are subject to certain time limit. But in many applications regardless of network lifetime and power consumption of nodes is the main objective sense timely delivery of data. In the first application of power reduction and the challenges ahead in the use of real-time communication support. Given the above issues requires a mechanism which can satisfy the different needs of the different applications may be felt in wireless sensor networks.

5. Conclusion

In this study, the genetic algorithm approach is used in order to enhance detection schemes of intrusion used in wireless sensor networks. Performance monitoring will devote plan to assess the suitability of the sensor nodes based on integrity, remaining battery power, and assigns coverage. Decentralized regulate the scheme because local monitoring node in the distribution network is optimized driving profile data is fed to the base station. The profiles of the input / output depending on the traffic pattern, delay profiles, and RSSI based position estimation are neighboring nodes. Information collected are processed at the base station along with other specific data using synchronization nodes messages and correlation analysis of the data collected. This approach can rapidly detect compromised nodes increases to 50 percent. Additionally, it complements the security mechanism [7] is a security feature based on a detailed analysis of the threats received as measured by the base station can be optimized. To offset the overhead monitor, an adaptive sampling depends on a variety of measures to implement a profile has been established. One limitation is that if we increase the number of nodes, the convergence time of genetic algorithm increases exponentially. Future work includes improving the scalability of the algorithm as we increase the number of nodes.

Reference

[1] B. Choi, E. Cho, J. Kim, C. Hong, and J. Kim, "A Sinkhole Attack Detection Mechanism for LQI based Mesh Routing in WSN", Information Networking, ICOIN International Conference on, pp.1-5, Jan 2009.

[2] V. Katiyar, N. Chand, and S. Soni, "Clustering Algorithms for Heterogeneous Wireless Sensor Network: A Survey", International Journal of Advanced Networking and Applications, Vol.2, No.4, pp.745–754, 2011.

[3] J. Kim and T. Cho, "Routing Path Generation for Reliable Transmission in Sensor Networks Using GA with Fuzzy Logic Based Fitness Function", Lecture Notes in Computer Science, Vol.4707, pp.637-648, 2007.

[4] B. Choi, E. Cho, J. Kim, C. Hong, and J. Kim, "A Sinkhole Attack Detection Mechanism for LQI based Mesh Routing in WSN", Information Networking, ICOIN International Conference on, pp.1-5, Jan 2009.

[5] H. Deng, X. Sun, B.Wang, and Y. Cao, "Selective Forwarding Attack Detection using Watermark in WSNs", CCCM 2009. ISECS International Colloquium on, pp.109-113, 2009.

[6] G. Acs, and L. Buttyan, "Dessiging a Secure Label-Switching Routing Protocol for Wireless Sensor Networks", Telecommunications Budapest University of Technology and Economics, Hungary, Dec.22, 2008.

[7] A. Modirkhazen, N. Ethnic, and O. Ibrahim, "Empirical Study on Secure Routing Protocols in Wireless Sensor Networks", International Journal of Advancements in Computing Technology, Vol.2, No.5, Dec 2010.

[8] Y. Li, S. Chen, C. Song, Z. Wang, and Y. Dun, "Enhancing Teal-Time Delivery in Wireless Sensor Networks with Two-Hop Information", IEEE Trans. On Industrial Informatics, Vol.5, No.2, 2009.

[9] I. Dtojmenovic, "Handbook of Sensor Network: Algorithms and Architectures", New York: Wiley, 2005.

[10] J. Hill, R. Szewczyk, A. Woo, S .Hollar, D. Culler, and K. Pister, "System architecture directions for networked sensors", ACM Sigplan Notices, Vol.35, pp.93-104, 2000.

[11] I. F. Akyldiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey", Computer Networks, Vol.38, pp.393-422, 2002.

[12] R. Khanna, H. Liu, and H. Chen, "Self-Organisation of Sensor Networks Using Genetic Algorithms", Int. J. Senor Network, Vol.1, NOS. ¾, 2006.

[13] G. Wenliang, S. Huichang, Y. Jun and Z. Yifei, "Application of Genetic Algorithm in Energy Efficient Routing", China-Japan Joint Microwave Conference, pp.737-740, 2009.

[14] L. Guo, and Q. Tang, "An Improved Routing Protocol in WSN with Hybrid Genetic Algorithm", Second International Conference on Network Security Wireless Communications and Trusted Computing (NSWCTC), Vol.2, pp.289-292, 2010.

[15] C. Sun, and T.Cho, "Path Selection Method for Reliable Data Transmission in Sensor Networks Using GA", IJCSNS International Journal of Computer Science and Network Security, Vol.11 No.2, Feb., 2011.

[16] J. M. Kim and T. H. Cho, "Routing Path Generation for Reliable Transmission in Sensor Networks Using GA with Fuzzy Logic Based Fitness Function", Lecture Notes in Computer Science, Vol.4707, pp.637-648, 2007.

[17] Al-Ghazal, M. Sayed, and A. Kelash, "Routing Optimization Using Genetic Algorithm in Ad Hoc Networks", The IEEE Symposium on Signal Processing and Information Technology (ISSPIT) Cairo, 2007.

[18] L. Guo, and Q. Tang, "An Improved Routing Protocol in WSN with Hybrid Genetic Algorithm", Second International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC), Vol.2, pp.289-292, 2010.