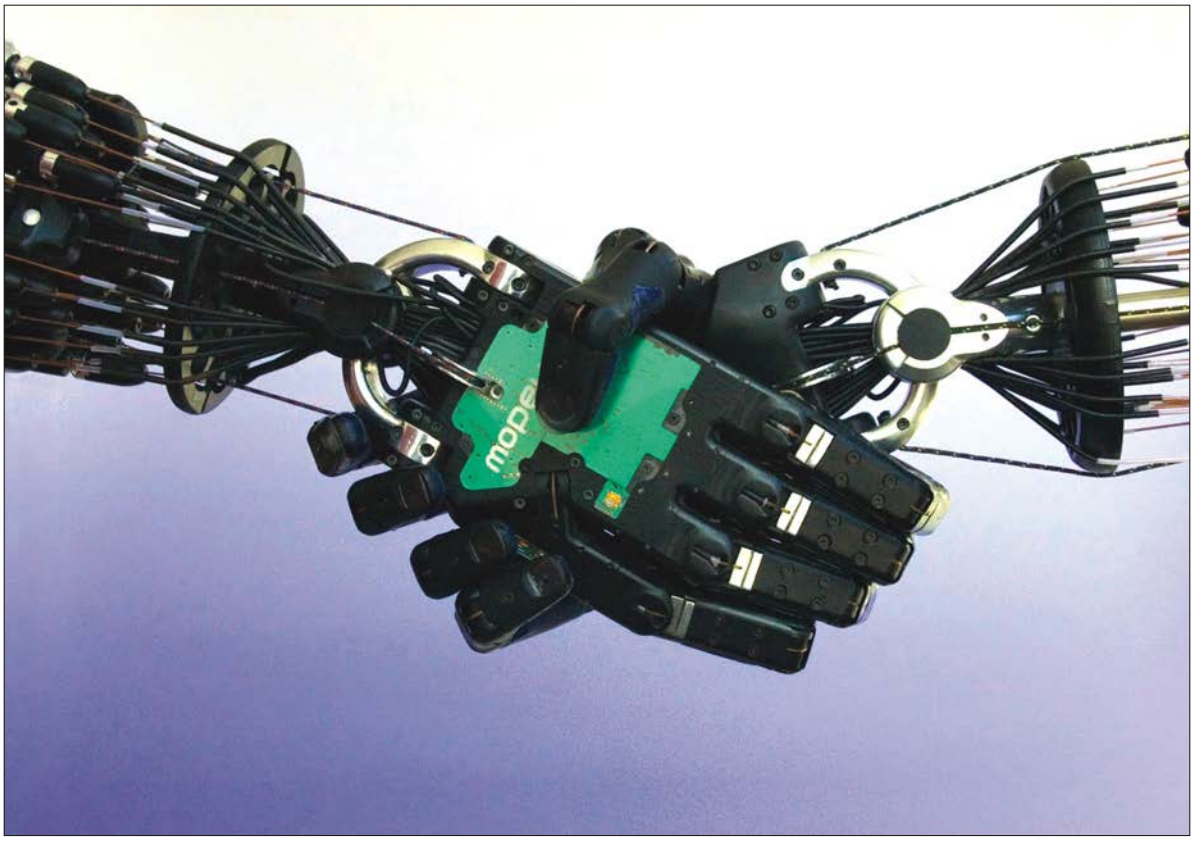

Journal of Artificial Intelligence

ISSN 1994-5450

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Artificial Intelligence 6 (2): 175-180, 2013
ISSN 1994-5450 / DOI: 10.3923/jai.2013.175.180

Sentry Based Intruder Detection Technique for Wireless Sensor Networks

[1]P. Arivubrakan and [2]V.R.S. Dhulipala

[1]M.E. Pervasive Computing Technologies, [2]Centre for Convergence of Technologies, Anna University of Technology, Tiruchirappalli, Tamil Nadu, India

Corresponding Author: P. Arivubrakan, M.E. Pervasive Computing Technologies, Anna University of Technology, Tiruchirappalli, Tamil Nadu, India

ABSTRACT

Wireless Sensor Networks consist of nodes with sensing, computation and wireless communications capabilities. Energy is the biggest constraint to wireless sensor capabilities. Sensor networks are increasingly being used in many applications where the communication between nodes requires to be protected from intruders. Local monitoring is an efficient mechanism for enhancing the security of multi-hop sensor networks. It can be overcome by the monitoring of the nodes. Many techniques have been proposed in the context of malicious nodes. In the sleep-wake schedule of nodes which are vulnerable to simple attacks and consumes more energy in sensor networks. In this study, a new technique has been introduced that takes part of communication which can be monitored using a sentry node and gathers the information from the neighbouring entity node within its transmission range or until it reach to the destination for providing a secured way of communication.

Key words: Sentry node, local monitoring, energy ,intruder, neighbour node, secured communication

INTRODUCTION

Wireless Sensor Networks (WSNs) is a network that has a huge number of sensor nodes to observe the environmental surroundings (Akyildiz *et al*., 2002). The sensing devices have modest power consisting of a controller for information processing, a chip and antenna for transmission and a sensor for sensing an environment. The advance of WSNs was initially motivated by military applications. Military applications is to track the movement of intruders.

Sensor network has a numerous advantages but are resource constrained. Sensor nodes performs sensing; data storage, communication, monitoring and processing. It has been shown in the literature that local monitoring is a feasible mechanism to counter such attacks. In local monitoring, nodes monitor a portion of the traffic from neighbor nodes (Huang and Lee, 2003; Da Silva *et al*., 2005) and various checks are made in the vicinity to detect and identify any malicious behavior. For systems in which consensus is desired, each node initiates a protocol to broadcast an alarm and an algorithm is implemented. Many techniques have been introduced that use the framework of local monitoring to achieve specific tasks such as intrusion detection

(Khalil *et al*., 2005; Yrjola, 2005). Local monitoring ensures that packets are successfully reached to the destination without any delay (Hui *et al*., 2003; Schurgers and Srinivastawa, 2001; Nguyen *et al*., 2008; Liu *et al*., 2005; Chakrabarty *et al*., 2002). We introduce a technique for node detection in WSNs while performing monitoring without significantly degrading security performance (Sivaraman *et al*., 2009).

In this study, we introduce a sentry based Intrusion Detection Technique (SIDT) to monitor the node entry. Sensor nodes are classified into two categories, sentry and non-sentry. Sentry node is to monitor the communication with high energy and detects the malicious node in the network. The rest of the nodes in the network are called as a non-sentry node. The selection of the sentry is based on Sentry Selection Algorithm (SSA) which immense based upon a parametric concern.

PROPOSED TECHNIQUE

The proposed technique introduces a SIDT to perform monitoring in multi-hop wireless networks. Sensor networks consist of the source node, destination node, sentry node and non-sentry node. Sentry node is the sensor node provide sufficient coverage to perform continuous monitoring of the communication, remaining nodes are called as non-sentry node. It consumes the energy of the node by the idle state. Sentry node performs monitoring within its transmission range. Selection of the sentry node is based on Fig. 1.

The concept of SIDT is to detect the malicious nodes in the large scale scalable network. The Sentry node is to monitor, the new entry node and gathers the information about the node parameters and to decide the new entry node to be added in the scalable network. The proposed technique detects the intruder in the terrain and provides secured way of communication. WSN has limited energy due to the sensing capability. SSA attempt to reduce the total consumption of energy usage over all nodes, to prolong the capacity utilization and connectivity among all nodes (Dhulipala *et al*., 2010; Tian and Georganas, 2002). Sentry node is to monitor the transmission of the two nodes such as the source node and neighbour node within its range and keep on updating the node information of the neighbour node until it reaches to the destination node.

SSA is used to select the sufficient and suitable set of sentry that is required to monitor a certain communication link from the deployed nodes. The sensor nodes are aware of their deployment. The algorithm in itialize computation of energy and selection of the sentry is based on the highest energy as the sentry to monitor the communication within its range,

Step 1: Find the residual energy (RE)
Step 2: Calculate the highest energy from RE.
Step 3: Assign sentry node
Step 4: Perform monitoring
Step 5: If (Energy of the sentry<Energy of the non- sentry)
Compute the remaining energy
Go to step 2-4
Else
Repeat the process until it reaches to destination

Fig. 1: Sentry selection algorithm

while performing monitoring it drainsome energy and select the new sentry from the non-sentry remaining energy. If the computation energy of the sensor node decrease, it compute the residual energy by the simulation time (Zou and Zheng, 2010). If the residual energy of the node is same as the new computation residual energy, same sentry as sentry node (Kanagachidambaresan *et al.*, 2012).

The computation energy of the node is by the sensing power divide by time taken for the network for communication and are monitored by the sentry node. The sentry changes depending upon the residual energy. The Multi-hop communication consume more energy (Arivubrakan and Dhulipala, 2012).

SENTRY BASED MECHANISM

Figure 2 shows the sentry based mechanism consists of a sensor node in the network to perform monitoring. Sentry node has the highest energy to detect and authenticate the external nodes. In the multi-hop wireless network there is a possibility for the malicious node to interact with the communication in the network, it can be overcome by the sentry node.

Sentry node authenticates only the trusted node and provides secure communication within the transmission range. Sentry node lies at the perimeter of the network transmission range and detects the malicious node in the multi-hop network. Malicious node interaction in the network gives improper communication leads to more amount of packet loss. It can be overcome by the authentication of the sentry node. The sentry node detects the intruder node and protect it from the communication. The Fig. 3 shows the sentry node schematic diagram.

SIMULATION RESULTS

The performance has been analyzed with sentry and without sentry using Network Simulator (NS2). We compute the performance for selected metrics such as throughput and end to end delay Table 1 shows the simulation parameter.

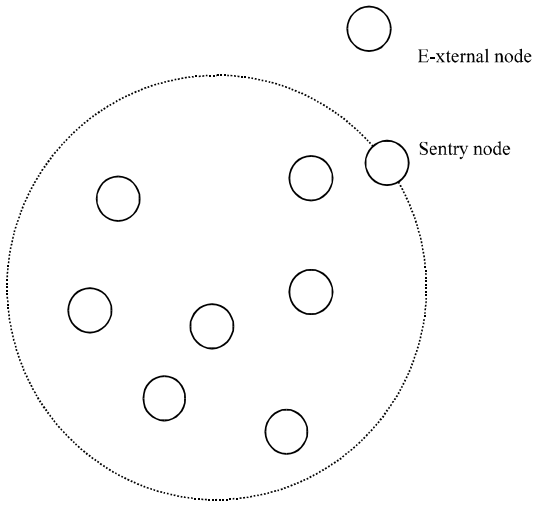

Fig. 2: Schematics of perimeter of network transmission range

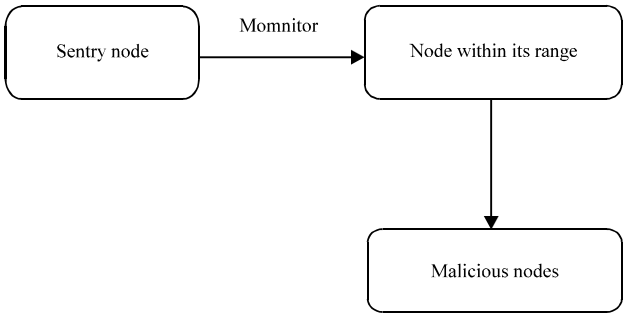

Fig. 3: Schematics of sentry node

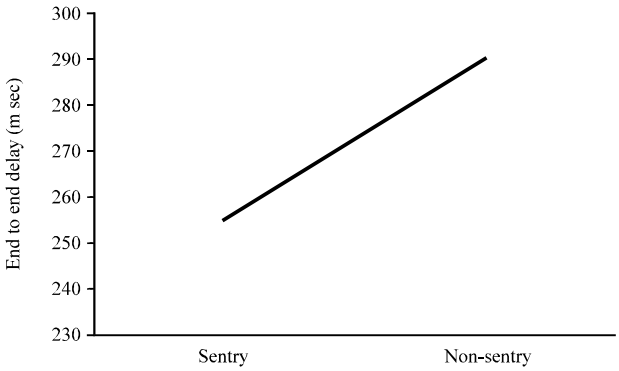

Fig. 4: End to end delay of sentry and non-sentry node

Table 1: Simulation parameter

Parameter	Value
Network simulator	Ns2.29
Interface queue type	Drop Tail/PriQueue
Routing protocols	(AODV) *Ad hoc* on-demand distance vector
MAC (Media Access Control)	802-11
Transmission range (m)	250
Traffic type	CBR (Constant Bit Rate)
Max packet in queue	50
Simulation time (m sec)	30

Parameter analysis

Average delay: Average delay is the difference of packets sent and received them by the total time. The Fig. 4 shows the delay for the sentry node and non-sentry node. Delay is low for the sentry node based network which reduced the energy consumption compared to the non-sentry node scenario which shows the efficacy of the proposed technique.

Throughput: Throughput defines the number of total packets arriving at the destination per second. The Fig. 5. shows the throughput provided by the sentry node with a transmission range of 30 m under CBR connection at simulation time 30 m sec^{-1}. Maximum Throughput is attained by authentication of sentry node.

Fig. 5: Throughput natrix

CONCLUSION

The sentry based intruder detection technique in WSN provides a secured way of communicating by detecting the malicious node and thereby protecting the network. The sentry based technique based on this work could be useful for achieving optimum throughput and will be helpful in scalable communication process. In the future, we plan to extend the technique by involving more performance metrics with suitable specification.

REFERENCES

Akyildiz, I.F., W. Su, Y. Sankarasubramaniam and E. Cayirci, 2002. Wireless sensor networks: A survey. Comput. Networks, 38: 393-422.

Arivubrakan, P. and V.R.S. Dhulipala, 2012. Energy consumption heuristics in wireless sensor networks. Proceedings of the IEEE International Conference on Computing, Communication and Applications, February 22-24, 2012, Dindigul, Tamilnadu, pp: 1-3.

Chakrabarty, K., S.S. Lyengar, H. Qi and E. Cho, 2002. Grid coverage for surveillance and target location in distributed sensor networks. IEEE Trans. Comput., 51: 1448-1453.

Da Silva, A.P.R., M.T.H. Martins, B.P.S. Rocha, A.A.F. Loureiro and L.B. Ruiz *et al.*, 2005. Decentralized intrusion detection in wireless sensor networks. Proceedings of the 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks, Oct. 13, ACM Press, Montreal, Quebec, Canada, pp: 16-23.

Dhulipala, V.R.S., V. Aarthy and RM. Chandrasekaran, 2010. Energy and fault aware management framework for wireless sensor network. Inform. Process. Manage., 70: 461-464.

Huang, Y. and W. Lee, 2003. A cooperative intrusion detection system for ad hoc networks. Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, October 31, 2003, New York, USA., pp: 135-147.

Hui, J.W., Z. Ren and B. Krogh, 2003. Sentry-based power management in wireless sensor networks. Proceedings of the 2nd International Workshop Information Processing in Sensor Networks, April 22-23, 2003, Palo Alto, CA.,USA., pp: 458-472.

Kanagachidambaresan, G.R., V.R.S. Dhulipala and M.S. Udhaya, 2012. Markovian model based trustworthy architecture. Procedia Eng., 30: 718-725.

Khalil, I., S. Bagchi and C. Nina-Rotaru, 2005. Dicas: Detection, diagnosis and isolation of control attacks in sensor networks. Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks, September 5-9, 2005, Athens, Greece, pp: 89-100.

Liu, S., K. Fan and P. Sinha, 2005. Dynamic sleep scheduling using online experimentation for wireless sensor networks. Proceedings of the 3rd International Workshop on Measurement, Modeling and Performance Analysis of Wireless Sensor Networks, July 21, 2005, San Diego, CA., USA.

Nguyen, L.T., X. Defago, R. Beuran and Y. Shinoda, 2008. An energy efficient routing scheme for mobile wireless sensor networks. Proceedings of the IEEE International Symposium on Wireless Communication Systems, October 21-24, 2008, Reykjavik, Iceland, pp: 568-572.

Schurgers, C. and M.B. Srinivastawa, 2001. Energy efficient routing in wireless sensor networks. Proceedings of the Military Communications Conference on Communications for Network-Centric Operations: Creating the Information Force, Volume: 1, October 28-31, 2001, Tysons Corner, McLean, USA., pp: 357-361.

Sivaraman, R., V.R.S. Dhulipala, V. Aarthy and K. Kavitha, 2009. Energy comparison and analysis for cluster-based environment in wireless sensor networks. Int. J. Recent Trends Eng., 2: 89-91.

Tian, D. and N.D. Georganas, 2002. A coverage-preserving node scheduling scheme for large wireless sensor networks. Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications, September 28, 2002, Atlanta, Georgia, USA, pp: 32-41.

Yrjola, J., 2005. Summary of energy efficiency communication protocol for wireless micro sensor networks. http://www.tcs.hut.fi/Studies/T-79.194/papers/yrjola_050316.pdf

Zou, M. and S. Zheng, 2010. Energy balancing routing algorithm based on HGACA in WSNs. Proceedings of the 2nd International Conference on Computer Engineering and Technology, Volume: 2, April 16-18, 2010, Chengdu, Southwest China, pp: 637-640.