ISSN 2277-3061
Volume 15 Number6
International journal of Computers and Technology

Secure and Distributed On-Demand Randomized Routing in WSN

[1]V. Upendran [2]R. Dhanapal
[1]Research Scholar,Department of Computer Science
Bharathiar University
Coimbatore
Tamil Nadu - India
uppy_srgm@yahoo.co.in
[2]Principal, K.C.S Kasinadar college of Arts and Science
Chennai – Tamil Nadu - India
drdhanapal@gmail.com

ABSTRACT

Security and energy efficiency is of paramount importance in a wireless sensor network. This is due to their vulnerable deployment conditions and battery based power. This paper presents a secure and distributed algorithm that generates routes on-demand in a wireless sensor network. Dynamic route generation is facilitated by PSO, a metaheuristic technique. Current network traffic in that route and charge contained in the candidate node are used as evaluation parameters along with the node distance, hence a huge reduction in the packet loss was observed. Experiments were conducted and it was observed that the proposed algorithm exhibits very low selection overhead and also provides distributed routs, which eventually lead to prolonged network lifetime.

Indexing terms/Keywords

Altruism; Particle Swarm Optimization; Routing; Security; Selfishness; Wireless Sensor Networks

INTRODUCTION

Wireless Sensor Networks (WSN) have been very widely used in the recent times and has attracted several researches into this domain [13]. With the advancement in technology, WSNs are being used in several areas such as military [14], environmental applications [15], locating forest fires [16], observing animal habitats [17] and health care [18]. WSNs, though being very useful, are prone to failures and are vulnerable. The most important vulnerability arises from the fact that they are deployed mostly in inaccessible areas, hence cannot be frequently monitored. Once deployed, they function on their own. This makes the sensor nodes prone to several compromise based attacks. Further, the nodes in sensor networks do not have a dedicated power supply, instead they operate on batteries. Hence power also remains to be the most precious resource of a sensor node.

Reason for the increased importance given to the node's charge is that power contained in nodes determine the behavior of the nodes. Two prominent behaviors of sensor nodes include altruistic behavior and selfish behavior. When a node is initially deployed, it has full charge, hence their behavior tends to be altruistic. The node participates in generating and transferring its own packets and forwarding packets of other nodes. Every transmission causes a reduction in charge in the node. As the network operates, some nodes are operated on more than others, hence charge in certain nodes begin to deplete faster. This leads to the nodes turning selfish. Selfish nodes do not participate in packet forwarding, instead they only transfer their own packets. This behavior is incorporated in-order to retain the node from completely getting depleted.

The above mentioned properties are specific to WSNs and hence a routing algorithm designed for WSN should consider these properties and not just the shortest routing path to determine routes. There always exists a tradeoff between security and energy efficiency. This tradeoff is determined by the type of application the WSN is being designed to be operated on. This paper presents a randomized routing technique using PSO that generates dynamic random routes during transmissions. The routes are usually distributed throughout the network, hence specific node based charge depletions are avoided. Further, the dynamic on-demand routes provides security to the transmitted data.

The remainder of this paper is structured as follows; section II provides the related works, section III presents an elaborate discussion on the proposed approach, section IV presents the results and section V concludes the study.

RELATED WORKS

Wireless Sensor Networks (WSN), being a widely used technology has several contributions dealing with providing improvements in transmission security. Some of the recent contributions are discussed below.

A Bayesian Signaling Game model is presented in [1] that analyzes the strategy profiles for normal and anomalous nodes. This method also involves payoffs to motivate the nodes in abstaining them from malicious behavior. This is a variant of the trust based approach, where every node identifies and maintains the belief levels of their neighbors. These levels are periodically updated to provide effective results. The downsides of this approach is that it has high computational complexities, which makes them suitable only for the high performance based networks. Similar profiling based methods include [8]. Contributions by Roy et al. [2] served as the base for game theory based approaches. This method analyzed the usage of game theory on networked applications. Approaches that can be used to apply game theory concepts in network security was presented in [3].

A scalable and secure routing technique that uses the received signal strength in WSNs to perform effective routing is presented in [4]. A distributed location verification algorithm is used to identify the signal strength. This helps avoid spoofing attacks to a large extent. Scalability is provided by utilizing the broadcast nature of the WSN. The ambient trust model is also incorporated in this architecture to avert several other attacks. Several other location based techniques [5-7] are available that avert spoofing attacks using the signal strength of the received packets to identify the location of the transmitting node.

A node habit based routing technique is presented in [12]. This method analyzes and records the behavior of nodes in a network. These behavior patterns are used to perform the node selection process. Privacy of the nodes are preserved using cryptographic techniques. This is an on-demand routing algorithm that best operates on delay tolerant data. other on-demand routing techniques are discussed in [9-11].

SECURE AND DISTRIBUTED ON-DEMAND RANDOMIZED ROUTING IN WSN

Security and energy efficiency is of paramount importance in a wireless sensor network. The proposed approach presents an on-demand routing technique that uses randomized routing to provide security. Further, due to the process of randomized node selection, this method provides effective distribution of load, hence increasing the lifetime of the network. Figure 1 presents the architecture of the proposed methodology.

A wireless sensor network is a dynamic structure that must be flexible in order to accommodate network structure changes. Sensor nodes are prone to failures, hence the network details must be frequently updated. Since the proposed approach for routing requires the details of neighbor nodes, a hello packet is transmitted to all the 1-hop neighbors and their acknowledgements are collected to update the current live node list in the network and their current position. It becomes mandatory for every node to maintain the updated list in-order to avoid failed transmissions, since failed transmissions tend to be much costlier in WSNs when compared to normal networks.

On initiation of transmission, the packets are constructed and PSO based routing is initialized by the architecture. PSO [19], being a metaheuristic algorithm is a valid candidate for providing distributed routes. The randomness involved in PSO provides effective random routes that aids in the uniform use of energy in the network rather than usage of certain specific nodes. Another major problem in WSNs tend to be lack of memory and computational resources. PSO, when compared to other meta-heuristic techniques tend to utilize lesser memory and also has a low computational overhead [20].

On obtaining a transmission initiation signal, PSO builds the search space. The search space of PSO is composed of the current node and all the neighbor nodes and their corresponding properties [21]. This method considers the current network traffic recorded in that route and the current charge of the node. Utilizing a route with heavy traffic will often lead to transmission failures, while opting for a node with low charge will lead to the node turning selfish, which has a bad effect on the network's overall functioning. These two properties remain to be the most important properties governing safe transmission and in maintaining network stability. Hence they are used as components during the node selection phase.

All the required particles are distributed on the current node and the particle best (pbest) and global best (gbest) values are set to the current node. The initial velocity of a node must be assigned in-order to initiate movement in the search space. The initial velocity calculation is performed in a random manner and is maintained to be within the bounds of the current search space.

$$V_i \sim U(-|b_{up} - b_{lo}|, |b_{up} - b_{lo}|) \quad (1)$$

where b_{lo} and b_{up} are the lower and upper bounds of the search space respectively.

Particle acceleration is then triggered and the particles start their movement using the initial velocity and direction obtained from the previous phase. After the initial movement, the particles are distributed in the search space. PSO is continuous in nature, while the current application demands a discrete node as a solution. Hence a discretization function is used to identify the final node.

$$P' = \min\left(\sum_{j=1}^{n}\left(\sum_{k=1}^{d}\sqrt{(P_{ik} - N_{jk})^2}\right) \forall i = 1 \; to \; p\right) \quad (2)$$

where P_{ik} refers to the particle i's current location corresponding to dimension k, N_{jk} refers to the k^{th} dimension of node N_i.

This process is repeated for all particles and further movements are triggered by

$$V_{i,d} \leftarrow \omega V_{i,d} + \varphi_p r_p(P_{i,d} - X_{i,d}) + \varphi_p r_p(g_d - X_{i,d}) \quad (3)$$

Where r_p and r_g are the random numbers, $P_{i,d}$ and g_d are the parameter best and the global best values, $X_{i,d}$ is the value current particle position, and the parameters ω, φ_p, and φ_g are selected by the practitioner.

The *gbest* obtained after satisfying the termination criterion is considered as the next probable node for transmission of the packet. This process is repeated until the packet reaches the destination node.

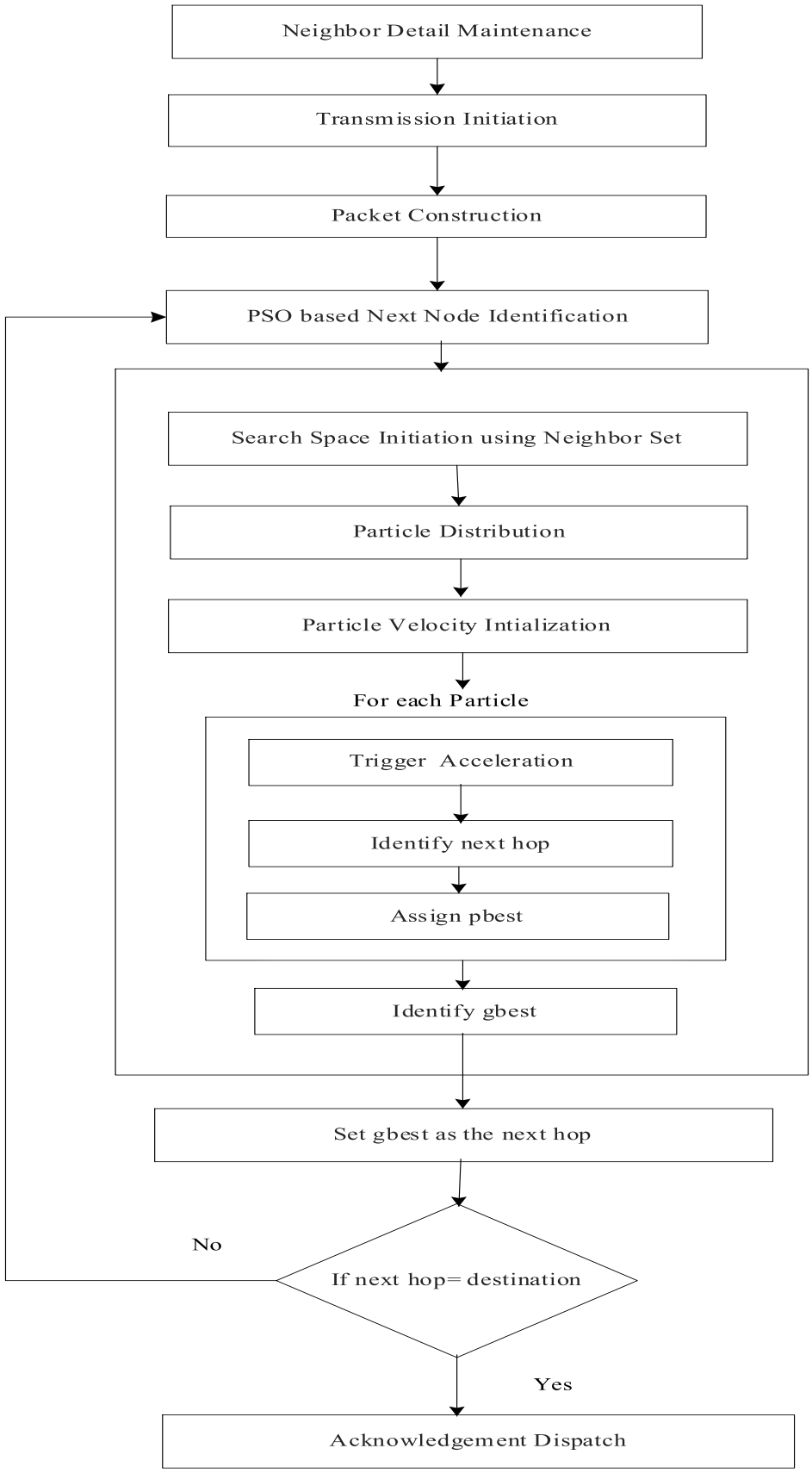

Fig 1. Secure and Distributed On-Demand Randomized Routing in WSN – Architecture

RESULTS AND DISCUSSION

Experiments were conducted on a network and the efficiency of the algorithm was measured in terms of selection overhead and load distribution among the nodes.

Fig 2. Selection Overhead

Fig 2 shows the selection overhead incurred in the path selection process. It shows the time taken to identify a complete path in the network for traversing all the nodes. It could be observed that the average time taken to traverse all the nodes in the network is approximately 6.5ms.

Fig 3. Total Path Covered

Fig 3 shows the total distance covered by the algorithm while traversing all the nodes in the network. It was observed that a minimum distance of 470 and a maximum distance of 565 was taken by the algorithm. This increase in the distance is attributed to the load distribution component in the algorithm.

Fig 4. Selection Overhead for Specific Path

Fig 4 presents the selection overhead for the algorithm to traverse between two specific nodes. It was observed that a maximum overhead of 6ms and a minimum overhead of 0ms was observed.

Fig 5. Distance Covered for Specific Path

Fig 5 shows the distance covered by the algorithm for traversing a specific path. It was observed that the distance covered ranges from 50 to 370. This is also attributed to the dispersion mechanism in the algorithm to help in load distribution and avoid selfish nodes in the network.

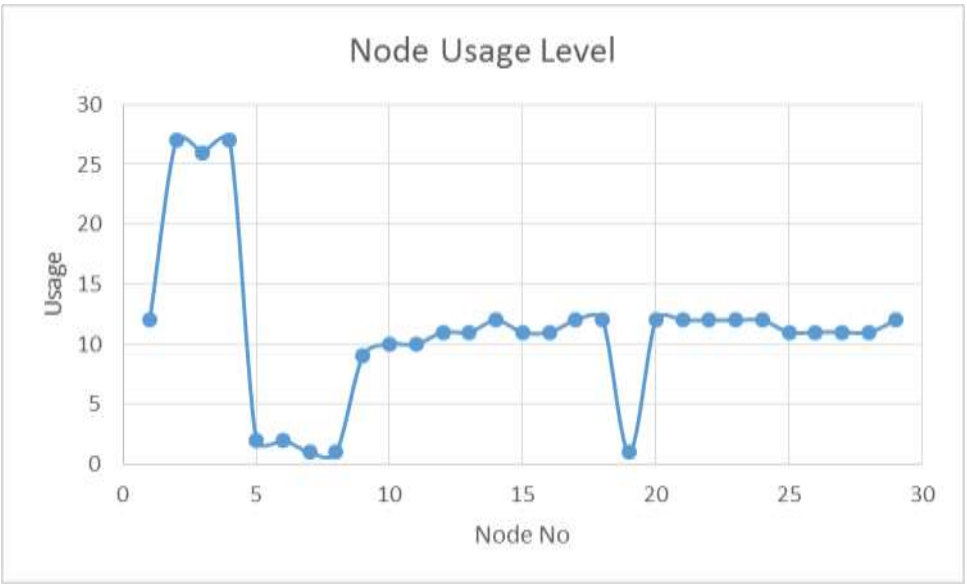

Fig 6. Node Usage Levels (Load Distribution)

Fig 6 shows the load distribution in the network for obtaining a path between specific nodes. The highest path access has occurred in the starting and ending nodes, while other nodes exhibit an average access throughout. For this experiment, the start and the end nodes are set to node 2 and node 4 respectively. Hence high access is observed in those nodes, while other nodes exhibit an average access. Hence it could be concluded that the proposed algorithm functions well in the distribution of load.

CONCLUSION

Several techniques exist in literature to perform secure communications in WSN. Some of these techniques also incorporate energy efficiency, but most of them are application specific. This paper presents a generic approach that provides both the major requirements of WSNs. The on-demand and dynamic nature of the algorithm has proved to be a major advantage when it comes to security and in maintaining the network's stability. Future extensions of this work includes utilizing a hybrid technique to reduce the selection overhead further. Though the selection overhead remains low, reducing it further will improve the ability of the algorithm to support real time traffic in the network. Further, trust levels of nodes can be recorded and incorporated into the algorithm to aid in the process of node selection, which can help prevent transmission failures to a large extent.

REFERENCES

[1] Kaliappan, M. and Paramasivan, B. 2015. Enhancing secure routing in Mobile Ad Hoc Networks using a Dynamic Bayesian Signalling Game model. Computers & Electrical Engineering 41: 301-313.

[2] Roy S, Ellis C, Shiva S, Dasgupta D, Shandilya V. and Wu Q. 2010. A survey of game theory as applied to network security. In: Proceeding of 43rd Hawaii international conference on system sciences. Honolulu, HI (USA): IEEE; p. 1–10.

[3] Manshaei MH, Zhu Q, Alpcan T, Bacsar T. and Hubaux J. 2013. Game theory meets network security and privacy. J ACM Comput Surveys-45(3):1–39.

[4] Lyu, Chen, Gu, D., Zhang, X., Sun, S., Zhang, Y. and Pande, A. 2015. SGOR: Secure and scalable geographic opportunistic routing with received signal strength in WSNs. Computer Communications 59: 37-51.

[5] Patwari, N., Ash, J.N., Kyperountas, S., Hero, A.O., Moses, R.L., Correal, N.S. 2005. Locating the nodes: cooperative localization in wireless sensor networks, IEEE Signal Process. Magaz. 22 (4) 54–69.

[6] Vaghefi, R.M., Gholami, M.R., Buehrer, R.M., Strom, E.G. 2013. Cooperative received signal strength-based sensor localization with unknown transmit powers, IEEE Trans. Signal Process. 61 (6)1389–1403.

[7] So, H.C. and Lin, L. 2011. Linear least squares approach for accurate received signal strength based source localization. IEEE Trans. Signal Process. 59 (8) 4035–4040.

[8] Sheng, Y., Tan, K., Chen, G. and Kotz, A. 2010. Campbell, Detecting 802.11 mac layer spoofing using received signal strength, in: Proceedings of INFOCOM 2008, IEEE, pp. 1768–1776.

[9] Hu, Y.C. Perrig, A. and Johnson, D.B. 2005. Ariadne: a secure on-demand routing protocol for ad hoc networks, Wirel. Netw. 11 (1–2) 21–38.

[10] Awerbuch, B., Curtmola, R., Holmer, D., Nita-Rotaru, C. and Rubens, H. 2008. Odsbr: an on-demand secure byzantine resilient routing protocol for wireless ad hoc networks, ACM Trans. Inf. Syst. Secur. 10 (4) 6:1–6:35.

[11] Yu, M., Zhou, M. and Su, W. 2009. A secure routing protocol against byzantine attacks for Manets in adversarial environments, IEEE Trans. Veh. Technol. 58 (1) 449.

[12] Sánchez-Carmona, Adrián, Robles, S. and Borrego, C. 2015. PrivHab+: A secure geographic routing protocol for DTN. Computer Communications.

[13] Rawat P, Singh K, Chaouchi H. and Bonnin J. 2014. Wireless sensor networks: a survey on recent developments and potential synergies. J Supercomput;68:1–48.

[14] Pathan AK, Hyung-Woo L, Choong-seon H. 2006. Security in wireless sensor networks: issues and challenges. In: Proceedings of the 8th international conference advanced communication technology (ICACT 2006). Phoenix Park, Korea; p. 1043-8.

[15] Sann Z. and Minn KT. 2011. Simulation of the rumor routing algorithm in sensor networks. In: Proceedings of the 3rd international conference on computer research and development (ICCRD. Shanghai, China; p. 10-4.

[16] Hefeeda M. and Bagheri M. 2007. wireless sensor networks for early detection of forest fires. In: Proceedings of the IEEE international conference on mobile adhoc and sensor systems (MASS 2007). Pisa, Italy; p. 1-6.

[17] Al Ameen M, Liu J, Kwak K. Security and privacy issues in wireless sensor networks for healthcare applications. J Med Syst 2010; 36:93–101.

[18] Alrajeh NA, Alabed MS, Elwahiby MS. 2013. Secure ant-based routing protocol for wireless sensor network. Int J Distrib Sens Netw.

[19] Kennedy, J. and Eberhart, R. 1995. Particle Swarm Optimization". Proceedings of IEEE International Conference on Neural Networks IV. pp. 1942–1948.doi:10.1109/ICNN.1995.488968.

[20] Shi, Y. and Eberhart, R.C. 1998. A modified particle swarm optimizer. Proceedings of IEEE International Conference on Evolutionary Computation. pp. 69–73.

[21] Eberhart, R.C. and Kennedy, J. 1995. A new optimizer using particle swarm theory, in: Proceedings of the Sixth International Symposium on Micro Machine and Human Science, IEEE Press, Piscataway, NJ, pp. 39–43.

Author' biography with Photo

Mr.V.Upendran is persuing his Ph.D in computer Science from Bharathiar University, Tamil Nadu, India. He is currently Head, Department of Computer Science, Srimad Andavan Arts and Science College (Autonomous), Affiliated to Bharathidasan University, Trichirappalli , India. He has 10 years of teaching experience. He has presented 2 International and 4 National papers in conferences. He has published 4 papers in International and one in National journal.

Prof.Dr.R.Dhanapal obtained his Ph.D in Computer Science from Bharathidasan University, Tamil Nadu, India. He has 29 years of teaching, research, administrative and industrial experience which includes 21 years of Government Service. He is currently Principal of K.C.S. Kasi Nadar College of Arts & Science Chennai, Tamil Nadu, India.

Besides being Professor, Administrator and researcher, he is also a prolific writer, having authored twenty one books on various topics in Computer Science. His books have been prescribed as text books in Bharathidasan University and Autonomous colleges affiliated to Bharathidasan University. He has served as Chairman of Board of Studies in Computer Science of Bharathidasan University, member of Board of Studies in Computer Science of several universities and autonomous colleges. Member of standing committee of Artificial Intelligence and Expert Systems of IASTED, Canada and Senior Member of International Association of Computer Science and Information Technology (IACSIT), Singapore and member of International Association of Engineers, Hongkong. He has Visited USA, Japan, Malaysia, and Singapore for presenting papers in the International conferences and to demonstrate the software developed by him. He is the recipient of the prestigious 'Life-time Achievement' and 'Excellence' Awards instituted by Government of India, 'Best Professor Award' Instituted by ASDF and Government of Puducherry.

He served as Principal Investigator for UGC and AICTE, New Delhi funded innovative, major and minor research projects worth of 1.7 crore especially in the area of Intelligent systems, Data Mining and Soft Computing. He is the recognized supervisor for research programmes in Computer Science leading to Ph.D and MS by research in several universities including Anna University Chennai, Bharathiar University Coimbatore, Manonmaniam Sundaranar University Tirunelveli, Periyar University Salem, Mother Teresa University Kodaikanal and many Deemed Universities. He has got 78 papers on his credit in international and national journals and 13 scholars obtained Ph.D under his guidance and supervision. He has been serving as Editor In Chief for the International Journal of Research and Reviews in Artificial Intelligence (IJRRAI) United Kingdom and serving as reviewer and member of editorial in accredited peer reviewed national and international journals including Elsevier Journals.