International Journal of Computer Science Engineering & Technology
APPROVED BY
NATIONAL SCIENCE LIBRARY (NSL)
NATIONAL INSTITUTE OF SCIENCE COMMUNICATION AND INFORMATION RESOURCES (NISCAIR)
COUNCIL OF SCIENTIFIC AND INDUSTRIAL RESEARCH (CSIR)- NEW DELHI INDIA .
ISSN :2455-9091

A NOVAL ANALYSIS OF ENEGY EFFICIENT AND TRUST BASED COOPERATIVE ROUTING IN NETWORKS

[1] D. Akila, [2] T. Keerthana, [3] N. Monisha, [4] A. Saranya, [5] Dr. R. J. Kavitha., M. E.,Ph. D
[1, 2, 3, 4] Research Scholar, [5] Assistant Professor,
[5] Department of ECE,
[1, 2, 3, 4, 5] University College of Engineering, Panruti.

ABSTRACT: Wireless sensor networks (WSNs) are increasingly being deployed in security-critical applications. Because of their inherent resource-constrained characteristics, they are prone to various security attacks, and a black hole attack is a type of attack that seriously affects data collection. In this paper, using recent advances in uncertain reasoning originated from artificial intelligence community. We propose a trust management scheme that enhances the security in networks name Hybrid and Efficient Intrusion Detection Systems (HEIDS). Here we used two frameworks for Trust Calculation and Decision Making process. The trust value is derived using Bayesian Inference, and Decision Making based on Dempster'-Shafer theory, which is a mathematical theory of evidence. In proposed process we add energy efficiency model by using Sleep Wake Scheduling technique in Trust method. We can achieve more energy consumption and high energy efficiency compared to previous Active Trust model.

Keywords: [Mobile Sensor networks, Hybrid and Efficient Routingalgorithm, Robust Routing, Efficient Data Gathering.]

1. INTRODUCTION

Wireless sensor networks (WSNs) are increasingly being deployed in security-critical applications. Because of their inherent resource-constrained characteristics, they are prone to various security attacks, and a black hole attack is a type of attack that seriously affects data collection. The adversary compromises a node and drops all packets that are routed via this node, resulting in sensitive data being discarded or unable to be forwarded to the sink. Because the network makes decisions depending on the nodes' sensed data, the consequence is that the network will completely fail and, more seriously, make incorrect decisions. Therefore, how to detect and avoid BLA is of great significance for security in WSNs. There is much research on black hole attacks. Such studies mainly focus on the strategy of avoiding black holes. Another approach does not require black hole information in advance. The Trust scheme is the first routing scheme that uses active detection routing to address BLA. The most significant difference between Trust and previous research is that we create multiple detection routes in regions with residue energy; because the attacker is not aware of detection routes, it will attack these routes and, in so doing, be exposed. In this way, the attacker's behavior and location, as well as nodal trust, can be obtained and used to avoid black holes when processing

real data routes. To the best of our knowledge, this is the first proposed active detection mechanism in WSNs.

Energy is very precious in WSNs, and there will be more energy consumption if active detection is processed. Therefore, in previous research, it was impossible to imagine adopting such high-energy-consumption active detection routes.

2. RELATED WORK

A Structured Approach to Optimization of Energy Harvesting Wireless Sensor Networks - Nicholas Roseveare, Balasubramaniam Natarajan -We analyze the data throughput maximization problem over fading channels for a energy harvesting wireless sensor network. The effective use of energy harvesting wireless sensor networks requires an apt understanding of the underlying environmental processes. Energy as a constrained resource must be carefully utilized so as to enable good performance through a horizon of epochs, trading off sensing performance and energy usage. We develop an algorithm for the allocation of power across sensors and time which is based on observations of the underlying structure of the optimization problem. We provide an analysis of particular features of the problem and present a maximum sum rate algorithm for generalized energy flow constraints, which proves to be optimal given known energy availability and fading coefficients. We present simulation results to validate the theory and algorithm.

Node Clustering in Wireless Sensor Networks: Recent Developments and Deployment Challenges- OssamaYounis, Marwan Krunz, Srinivasan - The large-scale deployment of wireless sensor networks (WSNs) and the need for data aggregation necessitate efficient organization of the network topology for the purpose of balancing the load and prolonging the network lifetime. Clustering has proven to be an effective approach for organizing the network into a connected hierarchy. In this article, we highlight the challenges in clustering a WSN, discuss the design rationale of the different clustering approaches, and classify the proposed approaches based on their objectives and design principles. We further discuss several key issues that affect the practical deployment of clustering techniques in sensor network applications.

Hierarchical routing in ad hoc mobile networks - Elizabeth M. Belding-Royer - Clustering is a method by which nodes are hierarchically organized on the basis of their relative proximity to one another. Routes can be recorded hierarchically, across clusters, to increase routing flexibility. Hierarchical routing greatly increases the scalability of routing in ad hoc networks by increasing the robustness of routes. This paper presents the Adaptive Routing using Clusters (ARC) protocol, a protocol that creates a cluster hierarchy composed of cluster leaders and gateway nodes to interconnect clusters. ARC introduces a new algorithm for cluster leader revocation that eliminates the ripple effect caused by leadership changes. Further, ARC utilizes a limited broadcast algorithm for reducing the impact of network floods.

Energy-Efficient Communication Protocol for Wireless Micro sensor Networks - Wendi Rabiner, Anantha Chandrakasan, HariBalakrishnan-Wireless distributed micro sensor systems will enable the reliable monitoring of a variety of environments for both civil and military applications. In this paper, we look at communication protocols, which can have significant impact on the overall energy dissipation of these networks. Based on our findings that the conventional protocols of direct transmission, minimum-transmission-energy, multihop routing, and static clustering may not be optimal for sensor networks, we propose LEACH (Low-Energy Adaptive Clustering Hierarchy), a clustering-based protocol that utilizes randomized rotation of local cluster base stations (cluster-heads) to evenly distribute the energy load among the sensors in the network. LEACH uses localized coordination to enable scalability and robustness for dynamic

networks, and incorporates data fusion into the routing protocol to reduce the amount of information that must be transmitted to the base station.

3. METHODOLOGIES

Wireless networks are increasingly being deployed in security-critical applications. Because of their inherent resource-constrained characteristics, they are prone to various security attacks, and a black hole attack is a type of attack that seriously affects data collection. In this paper, using recent advances in uncertain reasoning originated from artificial intelligence community.

We propose a trust management scheme that enhances the security in networks name Hybrid and Efficient Intrusion Detection Systems (HEIDS). Here we used two frameworks for Trust Calculation and Decision Making process. The trust value is derived using Bayesian Inference, and Decision Making based on Dempster'-Shafer theory, which is a mathematical theory of evidence. In proposed process we add energy efficiency model by using Sleep Wake Scheduling technique in Trust method. We can achieve more energy consumption and high energy efficiency compared to previous Active Trust model.

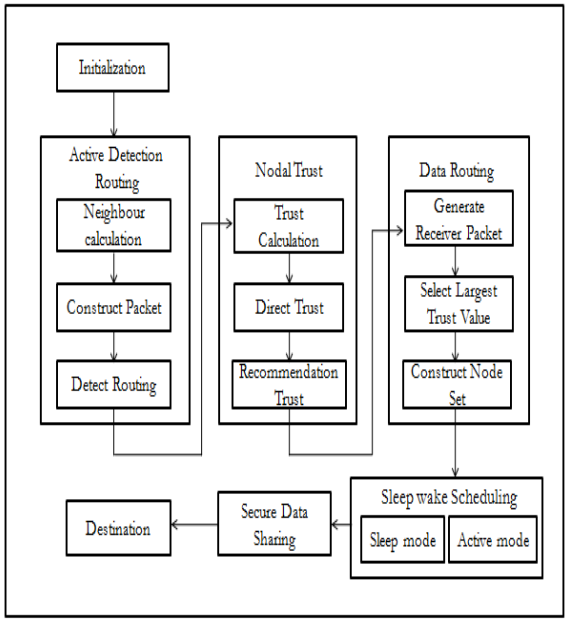


Figure 3.1 Proposed System

3.1 Active Detection Routing

A detection route refers to a route without data packets whose goal is to convince the adversary to launch an attack so the system can identify the attack behavior and then mark the black hole location. Thus, the system can lower the trust of suspicious nodes and increment the trust of nodes in successful routing routes. Through active detection routing, nodal trust can be quickly obtained, and it can effectively guide the data route in choosing nodes with high trust to avoid black holes.

In this scheme, the source node randomly selects an undetected neighbor node to create an active detection route. Considering that the longest detection route length is w, the detection route decreases its length by 1 for every hop until the length is decreased to 0, and then the detection route ends. This section details the implementation of the active detection routing protocol.

head	type	source	ϖ	ω	id

head	type	source	Destination	S-id	id

The feedback packet is routed back to the data source; because nodes cache the detection route info, the feedback packet is able to return back to the source, and the following is the algorithm for the detection route protocol.

3.2 Nodal Trust

During data routing and detection routing, every node will perform a nodal trust calculation to aid in black hole avoidance. When node A performs a detection route for node B at time it, if the detection data are successfully routed.

Nodal direction trust: Consider the trust set of node A to node B during t to be:Nodal recommendation trust: Node A is the trust evaluator, node C is the target of evaluation, and node B is a recommender of A.

Consider B A Cto be the direction trust of A to B and C BC to be the direction trust of

B to C; then, the recommendation trust of A to C is

$$R_A^C = C_A^B \times C_B^C$$

For the trust of multiple recommendations, the calculation of the recommendation trust from A to B, B to C, etc., until D to E is

$$R_A^E = C_A^B \times C_B^C \times C_C^D \times C_D^E$$

Recommendation trust merging: Consider that the recommender set of node A is AR, in ∈AR and that the recommendation trust of in to node K is , I k A R; then, the merged trust of A to K is

$$U_A^K = \sum_{n_i \in A_n} \left(u_{n_i} R_A^{n_i,k} \right) \; | u_{n_i} = \frac{R_A^{n_i,k}}{\left(R_A^{n_1,k} + R_A^{n_2,k} + \ldots + R_A^{n_{m-1},k} + R_A^{n_m,k} \right)}$$

Comprehensive trust: Comprehensive trust is the total trust, which merges the recommendation trust and direction trust: The comprehensive trust of a node can be computed as follows. After the node launches a detection route, it calculates the direction trust according to Eq. For each receivedfeedback packet. Through interactions, the node obtains the recommendation trust from its neighbors according. Finally, it calculates the comprehensive trust according.

3.3 Data Routing

The data routing refers to the process of nodal data routing to the sink. The routing protocol is similar to common routing protocols in WSNs; the difference is that the route will select a node with high trust for the next hop to avoid black holes and thus improve the success ratio of reaching the sink.

The core idea of data routing is that when any node receives a data packet, it selects one node from the set of candidates nearer the sink whose trust is greater than the preset threshold as the next hop. If the node cannot find any such appropriate next hop node, it will send a feedback failure to the upper node, and the upper node will re-calculate the unselected node set and select the node with the largest trust as the next hop; similarly, if it cannot find any such appropriate next hop, it sends a feedback failure to its upper node. The upper node, working in the same manner, will re-select a different node from among its neighbors nearer the sink until the data are routed to the sink or there is conclusively no path to the sink.

3.4 Sleep wake scheduling

In this module used to initialize the nodes in network topology. We used network topology and topography for our network animator window (network window). We have syntax for create nodes in network animator window. Sensors that are active or asleep are called as surviving sensors and sensors that are malfunctioned or deadlines are called to fail. Sensor modes vary, based upon the active sensors vary at each and every time. So, in this work we propose a method to decide a sleep schedule at each and every key time. The 1st key time is the initial time, at which each sensor is works with the initial battery power. Here the sleep schedule is initialized. During the 1st key if some targets are not covered mean the 2nd key time is started. At the 2nd key time, the sensors information is updated and sleep schedule is followed to cover all targets. Similarly, the 3rd key time, 4th key time and so on can be followed. And, a sleep schedule is followed at each key time until survival sensors cannot cover all targets.

4. EXPERIMENTAL RESULT AND DISCUSSION

PERFORMANCE ANALYSIS:

This research work used ns-2 as the network simulator and conducted numerous simulations to evaluate the HEIDSperformance. All sensor nodes are randomly scattered with a uniform distribution. The location of the sink is randomly determined. This study evaluates the routing performance under scenarios with different numbers of sensor nodes.

This research work evaluates the following main performance metrics:

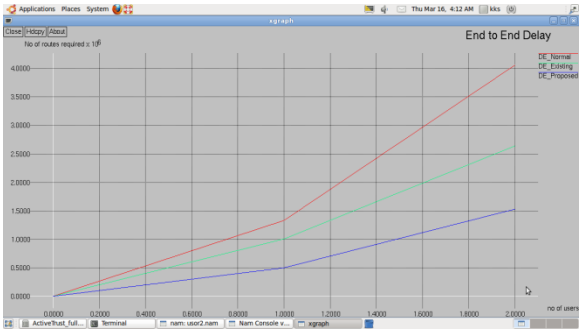
1) Packet Delivery ratio: measures the mean rate of the packet sending and receiving then calculate delivery ratio.

2) Energy consumption: Means Reduce the usage of energy level in network, and here improves energy efficiency rate.

3) End-to-end Delay: means the time delay experienced by the source node while transmitting a report message to the sink.

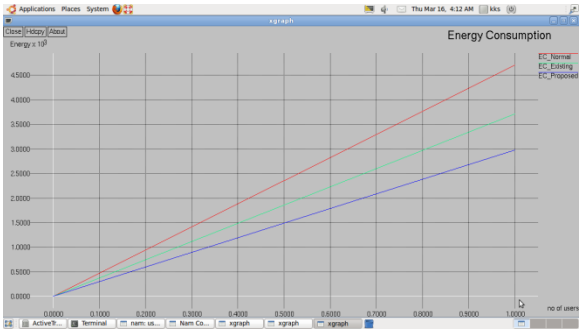
4) Throughput ratio: Measures data sharing and successive ratio rate.

4.1. Delay ratio:



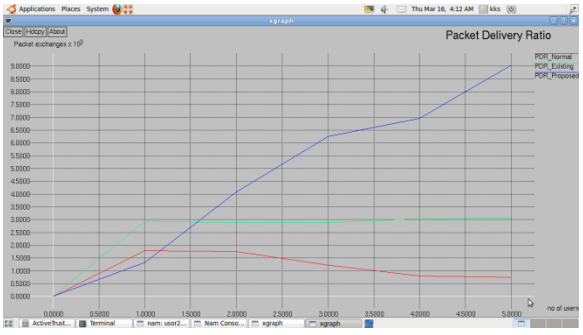
Above figure mention delay ratio of our proposed and existing comparison.

4.2. Energy Consumption rate:



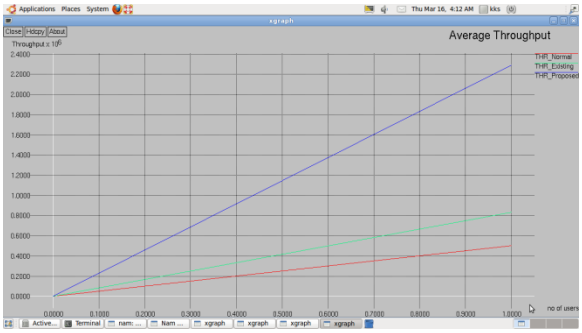
Above figure mention energy consumption ratio of our proposed and existing comparison.

4.3. Packet Delivery Ratio:



Above figure mention Packet Delivery Ratioof our proposed and existing comparison.

4.4. Throughput ratio:



Above figure mention Throughput ratio of our proposed and existing comparison.

CONCLUSION

In this paper, we have proposed a novel security and trust routing scheme based on active detection, and it has the following excellent properties: (1) High successful routing probability, security and scalability. The ActiveTrust scheme can quickly detect the nodal trust and then avoid suspicious nodes to quickly achieve a nearly 100% successful routing probability. (2) High energy efficiency. The ActiveTrust scheme fully uses residue energy to construct multiple detection routes. The theoretical analysis and experimental results have shown that our scheme improves the successful routing probability by more than 3 times, up to 10 times in some cases. Further, our scheme improves both the energy efficiency and the network security performance. It has important significance for wireless sensor network security.

REFERENCE

[1]. N. Roseveare and B. Natarajan, “A structured approach to optimization of energy harvesting wireless sensor networks”, IEEE Consumer

Communications and Networking Conference (CCNC), pp. 420-425, Las Vegas, 2013.

[2]. O. Younis, M. Krunz and S. Ramasubramanian, ”Node clustering in

wireless sensor networks: recent developments and deployment challenges", IEEE Network, Vol. 20, No.3, pp. 20-25, 2006.
[3]. C.E. Perkins, E.M. Royer, "The ad hoc on-demand distance vector protocol", Ad hoc networking, Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, pp. 173-219, 2001.
[4]. E. Belding-Royer, "Hierarchical routing in ad hoc mobile networks",Wireless Communications and Mobile Computing, Vol.2, No.5, pp. 515-532, 2002.
[5]. M. Lotfinezhad and B. Liang, "Effect of partially correlated data on clustering in wireless sensor networks", Proceedings of the IEEE
International Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON), Citeseer, pp.172-181, 2004.
[6]. A.A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks", Computer Communications, Vol. 30, pp. 28262841, 2007.
[7]. W. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energyefficient communication protocol for wireless microsensor networks", Proceedings of the 33rd Hawaii International Conference on System Sciences, Vol. 8, Citeseer, pp. 802, 2000.
[8]. I. Gupta, D. Riordan and S. Sampalli, "Cluster-head election using fuzzy logic for wireless sensor networks", Proceedings of the IEEE 3rd Annual Communication Networks and Services Research Conference, pp. 255-260, 2005.
[9]. A. Alchihabi, A. Dervis, E. Ever and F. Al-Turjman, "A Generic Framework for Optimizing Performance Metrics by Tuning Parameters of Clustering Protocols in WSNs", Wireless Networks, pp. 1-16, doi:10.1007/s11276-018-1665-8, 2018.
[10]. J. Kim, S. Park, Y. Han and T. Chung, "CHEF: cluster head election mechanism using fuzzy logic in wireless sensor networks", Proceedings of the IEEE 10th International Conference on Advanced Communication Technology (ICACT), pp. 654-659, 2008.
[11]. C.F. Li, M. Ye, G.H. Chen and J. Wu, "An energy-efficient unequal clustering mechanism for wireless sensor networks", Proceedings of
the 2nd IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS), pp. 604-611, Washington DC., 2005.
[12]. S. A. Sert, H. Bagci and A. Yazici, "MOFCA: Multi-objective fuzzy clustering algorithm for wireless sensor networks", Applied Soft Computing, Vol. 30, pp. 151-165, 2015.
[13]. Xuxun L, "A survey on clustering routing protocols in wireless sensor networks", Sensors Journal, Vol.12, No.8, pp. 11113-11153, doi:10.3390/s120811113, 2012.
[14]. O. Younis and S. Fahmy, "Distributed clustering in ad hoc sensor networks: a hybrid, energy-efficient approach", Proceedings of the IEEE 23rd Joint Annual Conference of Computer and Communications Socities (INFOCOM), Hong Kong, Vol.1, 2004; an extended version
appeared in IEEE Transactions Mobile Computing, Vol. 3, No. 4, pp. 366-379, 2004.
[15]. H. Ali, W. Shahzad, F. Khan, "Energy-efficient clustering in mobile ad-hoc networks using multi-objective particle swarm optimization", Applied Soft Computing, Vol. 12, pp. 1913-1928, 2012.
[16]. Z. Xu, Y. Yue and J. Wang, "A Density-based energy-efficient clustering algorithm for wireless sensor networks", International

Journal of Future Generation Communication and Networking, Vol. 6, No. 1, pp. 75-85, 2013.
[17]. P. Sasikumar and Shilpa, “Dynamic Power Control Clustering Wireless Sensor Networks Based on Multi-Packet Reception”, Indian Journal of Science and Technology, Vol. 9, No. 37, doi:10.17485/ijst/2016/v9i37/102120, 2016.
[18]. P. Nayak and A. Devulapalli, “A Fuzzy Logic-Based Clustering Algorithm for WSN to Extend the Network Lifetime”, IEEE Sensors Journal, Vol. 16, No. 1, 2016.
[19]. Online, URL:”WikiPedia Optimization”, Last Accessed: March 2017.
[20]. R. W. Eglese, “Simulated annealing: a tool for operational research”, European Journal of Operational Research, Vol. 46, No. 3, 271-281,
1990.
[21]. H.-J. Zimmermann. Fuzzy Set Theory and Its Applications. FourthEdition, Kluwer Academic Publishers Group, 2001.
[22]. Online, URL:”Castalia Simulation Platform”, Last Accessed: June 2017.