IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 3, March 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003062

Multi-Party Secret Key Concurrence Over State Dependent Wireless Transmit Channels

E. Sharmila,[1] Mrs. M. Malathi, M.C.A., M.Phil.,[2]Dip(Yoga)

Research Scholar, Department of Computer Science, Trinity College for Women, Namakkal, Tamilnadu, India[1]

Assistant Professor, Department of Computer Science, Trinity College for Women, Namakkal, Tamilnadu, India[2]

ABSTRACT: In recent years, as WSNs (Wireless Sensor Networks) are gentle broadly, multiple overlapping WSNs constructed on the similar area develop into more familiar. In such a situation, their lifetime is predictable to be extended by supportive packet forwarding. while some researchers have considered about support in multiple WSNs, most of them operate not consider the heterogeneity in characteristics of each WSN such as battery power, function start time, the quantity of nodes, nodes locations, energy utilization, packet size and/or data communication timing, and so on. In a heterogeneous environment, naive lifetime improvement with collaboration may not be fair. In this paper, we propose a fair supportive routing process for heterogeneous overlapped WSNs. It introduces an energy pool to maintain the total amount of energy consumption by cooperative forwarding. The energy pool plays a role of broker for fair cooperation. Finally, reproduction results show the excellent concert of the proposed method.

KEYWORDS: Sensor Network, Cooperative Routing, Fairness, Heterogeneous Environment, Load Balancing.

I. INTRODUCTION

Wireless sensor networks (WSNs) are composed of tiny battery-powered sensor nodes that have limited storage and radio capabilities. Therefore, for WSNs to remain operational for a long time, much attention has to be paid to energy consumption in the nodes. In a typical WSN, sensor nodes acquire and send data to a processing center called the sink. Because all data are forwarded to a sink, nodes around the sink tend to transmit many more packets than the others. In this case, the energy of such nodes will exhaust earlier than that of other nodes, causing an “energy hole” to appear around the sink. No more data can be delivered to the sink after the hole appears. Consequently, the energy remaining in the rest of the network is wasted, and the network lifetime is shorter than it could. In some applications, a WSN may comprise several thousand sensor nodes within an extended area (e.g., agriculture and environmental monitoring). In these cases, the diameter of the WSN may be some kilometers. To enable networks to be scalable, a WSN is typically subdivided into clusters and the data collected by cluster heads are sent to a sink. Clustering also supports data aggregation. This is a method by which data from multiple sensors are combined to eliminate redundant information and transmission, thereby reducing energy consumption. From another point of view, WSNs can be classified into two types, namely homogeneous and heterogeneous sensor networks. In a homogeneous WSN, all nodes have the same capabilities.

II. HEAVY-LOAD NODE AROUND A SINK

It is assumed that there are n WSNs in the same area. These WSNs have different applications. In addition, their start and finish times may differ, depending on each network’s requirements. The locations of the sinks in multiple WSNs are separated. Some nodes around a sink in one WSN may therefore be far from a sink in another WSN.

We focus on this fact in the proposed method, whereby a node that is far from a sink in its own network, but near a sink in another network, can forward a packet from a node in another WSN to the corresponding sink. In this paper, we call the former network the home network and the latter network the visitor network. The method achieves load balancing between a heavy-load node in a home network and a light-load node in a visitor network. As a result, the lifetime of both networks can be extended.

Specifically, each network constructs a path along which a node can’t forward a packet from a node in another WSN in advance. It is based on the well-known Ad hoc On-Demand Distance Vector (AODV) protocol), making it easy to implement. In addition, some nodes construct routes to the sinks of visitor networks.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003062

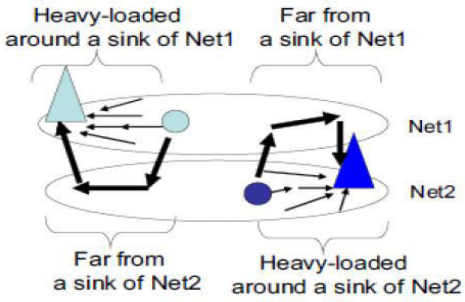

Figure 2.1: Heavy-load node around a sink

One WSN may therefore be far from a sink in another WSN. We focus on this fact in the proposed method, whereby a node that is far from a sink in its own network, but near a sink in another network, can forward a packet from a node in another WSN to the corresponding sink. In this paper, we call the former network the home network and the latter network the visitor network. The method achieves load balancing between a heavy-load node in a home network and a light-load node in a visitor network. As a result, the lifetime of both networks can be extended. Specifically, each network constructs a path along which a node can't forward a packet from a node in another WSN in advance. It is based on the well-known Ad hoc On-Demand Distance Vector (AODV) protocol), making it easy to implement. In addition, some nodes construct routes to the sinks of visitor networks.

III. METHODOLOGIES

3.1 COOPERATIVE ROUTING METHOD

In the proposed method, when a node sends its sensing data, it attaches the value of its residual energy in a header field of the packet. When a node relays a packet, it compares the residual energy of the node itself and that recorded in the packet, and the recorded value is replaced by smaller one. As a result, the minimum energy along the path from its source node is recorded. According to this procedure, a node can record a value of minimum energy along the paths every networks and select the path for the maximum value of this energy.

3.2 TRADITIONAL APPROACH FOR LONGER LIFETIME CLUSTERING

It is one of the most famous methods because of its good scalability and the support for data aggregation. Data aggregation combines data packets from multiple sensor nodes into one data packet by eliminating redundant information. This reduces the transmission load and the total amount of data. In clustering, the energy load is well balanced by dynamic election of cluster heads (CHs). By rotating the CH role among all sensor nodes, each node tends to expend the same amount of energy over time. Nevertheless, as with usual multi hop forwarding, a CH around a sink tends to have higher traffic than other CHs. As a result, nodes around sinks die earlier than other nodes, even in clustered WSN. In general, a single WSN has a single sink. The amount of traffic increases around the sink, therefore nodes around the sink tend to die earlier. This is called energy whole problem. Moreover, in a large-scale WSN with a large number of sensor nodes, the energy hole problem is more serious. Then, some researchers have proposed construction methods of multiple sink networks. In a multiple-sink WSN, sensor nodes are divided into a few clusters. Sensor nodes within a cluster are connected with one sink, which belongs to that cluster. In contrast to a single-sink WSN, in which nodes around the sink have to relay data from almost all nodes, nodes around each sink relay smaller amount of data only from nodes that are in the same cluster. Therefore, the communication load of nodes around sinks can be reduced. However, there are some problems such as how to determine the optimal location of each sink and the optimal number of sinks.

3.3 COOPERATION BETWEEN MULTIPLE WSNS

In existing studies, most researches assume that a single network is deployed by a single authority in the sensing area. However, as WSNs get utilized more widely, multiple WSNs tend to be deployed in the same area. For instance, in the UK, some different networks of cameras by different authorities such as police, highway patrol, and local city authorities are deployed on the same roads [18]. Recently, some researchers have proposed the cooperation method of multiple WSNs in such situations. When multiple WSNs are constructed in close proximity, they can help each other by forwarding data so that all networks involved benefit from collaborative effort. In the potential benefits of

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003062

cooperation in multiple WSNs are investigated. The authors formulated the system model with objective function and a set of problem constraints. Then, a linear programming framework is used to solve the optimization problem. Since their goal is to investigate the maximum achievable sensor network lifetime with different multi-domain cooperation strategies, optimization objective is network lifetime, which is defined as the time when the first sensor node in a network exhausts its battery and dies. The authors also investigated the cooperation in multiple networks that are deployed slightly different location. Some researchers have addressed the cooperation problem with using a game-theoretic framework. It is assumed that a WSN has a rational and selfish character and will only cooperate with another network if this association provides services that justify the cooperation. Virtual Cooperation Bond (VCB) Protocol is one of the game-theoretic approaches. It is a distributed protocol that makes different networks to cooperate, if and only if all the networks obtain some benefits by the cooperation. The authors formulated the cooperation problem among different WSNs as a cooperative game in game theory. In VCB protocol, the energy consumption of data communication is used as costs. When the cost gets higher, the payoff of a network gets lower. A sensor node and another node that belongs to another network forward a data packet coming from the other side, only if both networks can obtain the higher payoffs than no cooperation scenario. The simulation results showed that the VCB can save transmission energy between 20% and 30% in a certain environment.

3.4 NODE FUNCTION

As described above, the proposed method enables a node that is far from a sink in its home network, but near a sink in a visitor network, and can forward a packet from a node in the visitor network. Each node has a routing table that includes not only an entry for a sink in its home network but also an entry for a sink in the visitor network. When a node overhears a data packet from its visitor network, it decides whether to receive and forward it or to ignore it. This procedure is explained later in more detail.

3.5 ROUTING TABLE CREATION

This subsection explains how to create the routing table. Initially, each node sends an AODV-based route request packet to create an entry in its routing table for a sink in its home network. After this creation process, each node broadcasts an additional route request packet named B-REQ to the sinks of all visitor networks. (Nodes on the path from the node to the sink will create an entry in their routing table to the sink.) In addition, as a metric to decide the next hop, min Energy is also notified. This refers to the minimum residual energy of nodes along the path to the sink.

3.6 ROUTE DISCOVERY

Each sensor node creates its routing table based on a routing protocol. In this paper, we used ad hoc on-demand distance vector (AODV) [19] as a routing protocol, because AODV was developed for wireless ad hoc networks and was adopted for some WSN protocols such as Zigbee and ANT. In route discovery, each sensor node discovers its routes not only to the sink in its WSN but also to all the other sinks in the different WSNs for opportunities to forward data packets from nodes in different WSNs to their sink.

3.7 COOPERATIVE DATA FORWARDING

Since a sensor node has a single route toward the sink in its WSN, it forwards a data packet immediately to the next node on the route. On the other hand, a shared node sk has m routes for the sink via m networks, therefore it can choose an appropriate route for data forwarding. Since the lifetime of WSN depends on the lifetime of the energy-bottleneck nodes in the WSN, cooperative data packet forwarding via alternative nodes belonging to another's WSN.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003062

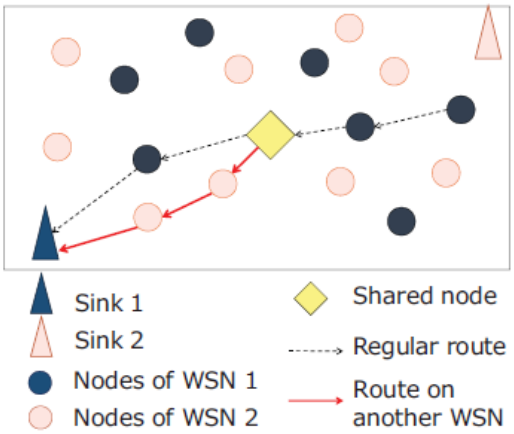

Figure: 3.7 Cooperative Data Forwarding

3.8 DISCUSSION ON THE CRYPTOGRAPHIC ANALYSIS

We do not make any assumption on the computational ability of the adversary, i.e., this leads to the unconditional secrecy in the cryptography terminology. Additionally, it is assumed that the channel state is random and not known by any party including the adversary a-priori. The adversary can hear the Alice's broadcast through a fading channel, and also the acknowledgments through a noise-free public discussion channel, i.e., we consider a passive eavesdropper that does not tamper with the communications of legitimate nodes. Furthermore, we assume all the legitimate nodes are authenticated so only these nodes can participate in the public discussion.

IV. GROUP SECRET KEY AGREEMENT OVER STATEDEPENDENT GAUSSIAN BROADCAST CHANNELS

In this section, by using the results derived in the previous sections, we will study the secret key generation capacity among multiple terminals having access to a state-dependent Gaussian broadcast channel. We will derive upper and lower bounds for the secret key generation capacity. Although, the proposed bounds are not matched in general, we will show that they will match in the high-dynamic range, high-SNR regime in a degree of freedom sense. Upper Bound for the Key Generation Capacity In order to upper bound the secrecy capacity for the Gaussian broadcast channel, we cannot apply the result of Corollary 1 directly because this result has been derived under the assumption that the transmitted and received symbols are discreet.

V. APPROACH FOR LONGER LIFETIME CLUSTERING

Is one of the most famous methods because of its good scalability and the support for data aggregation. Data aggregation combines data packets from multiple sensor nodes into one data packet by eliminating redundant information. This reduces the transmission load and the total amount of data. In clustering, the energy load is well balanced by dynamic election of cluster heads (CHs). By rotating the CH role among all sensor nodes, each node tends to expend the same amount of energy over time. Nevertheless, as with usual multi hop forwarding, a CH around a sink tends to have higher traffic than other CHs. As a result, nodes around sinks die earlier than other nodes, even in clustered WSN. In general, a single WSN has a single sink. The amount of traffic increases around the sink, therefore nodes around the sink tend to die earlier. This is called energy whole problem. Moreover, in a large-scale WSN with a large number of sensor nodes, the energy whole problem is more serious. Then, some researchers have proposed construction methods of multiple sink networks. In a multiple-sink WSN, sensor nodes are divided into a few clusters. Sensor nodes within a cluster are connected with one sink, which belongs to that cluster. In contrast to a single-sink WSN, in which nodes around the sink have to relay data from almost all nodes, nodes around each sink relay smaller amount of data only from nodes that are in the same cluster. Therefore, the communication load of nodes around sinks can be reduced. However, there are some problems such as how to determine the optimal location of each sink and the optimal number of sinks.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003062

5.1 UPPER BOUND FOR THE KEY GENERATION CAPACITY OF INDEPENDENT BROADCAST CHANNELS

The secret key generation capacity among multiple terminals (without eavesdropper having access to the broadcast channel) is completely characterized in . By using this result, it is possible to state an upper bound for the secrecy capacity of the key generation problem among multiple terminals where the eavesdropper has also access to the broadcast channel. This can be done by adding a dummy terminal to the first problem and giving the entire eavesdropper's information to this dummy node and let it to participate in the key generation.

5.2 GROUP SECRET KEY AGREEMENT OVER STATE-DEPENDENT GAUSSIAN BROADCAST CHANNELS

In this section, by using the results derived in the previous sections, we will study the secret key generation capacity among multiple terminals having access to a state-dependent Gaussian broadcast channel. We will derive upper and lower bounds for the secret key generation capacity. Although, the proposed bounds are not matched in general, we will show that they will match in the high-dynamic range, high-SNR regime in a degree of freedom sense.

5.3 UPPER BOUND FOR THE KEY GENERATION CAPACITY

In order to upper bound the secrecy capacity for the Gaussian broadcast channel, we cannot apply the result of Corollary directly because this result has been derived under the assumption that the transmitted and received symbols are discreet. However, the work in has extended the results of for continuous channels. we can write an upper bound for the secrecy capacity similar to Lemma 1 with the addition of a power constraint over the transmitted symbols.

VI. COOPERATION BETWEEN MULTIPLE WSNS

In existing studies, most researches assume that a single network is deployed by a single authority in the sensing area. However, as WSNs get utilized more widely, multiple WSNs tend to be deployed in the same area. For instance, in the UK, some different networks of cameras by different authorities such as police, highway patrol, and local city authorities are deployed on the same roads. Recently, some researchers have proposed the cooperation method of multiple WSNs in such situations. When multiple WSNs are constructed in close proximity, they can help each other by forwarding data so that all networks involved benefit from collaborative effort. In, the potential benefits of cooperation in multiple WSNs are investigated. The authors formulated the system model with objective function and a set of problem constraints. Then, a linear programming framework is used to solve the optimization problem. Since their goal is to investigate the maximum achievable sensor network lifetime with different multi-domain cooperation strategies, optimization objective is network lifetime, which is defined as the time when the first sensor node in a network exhausts its battery and dies. The authors also investigated the cooperation in multiple networks that are deployed slightly different location. Some researchers have addressed the cooperation problem with using a game-theoretic framework. It is assumed that a WSN has a rational and selfish character and will only cooperate with another network if this association provides services that justify the cooperation. Virtual Cooperation Bond (VCB) Protocol is one of the game-theoretic approaches. It is a distributed protocol that makes different networks to cooperate, if and only if all the networks obtain some benefits by the cooperation. The authors formulated the cooperation problem among different WSNs as a cooperative game in game theory. In VCB protocol, the energy consumption of data communication is used as costs. When the cost gets higher, the payoff of a network gets lower. A sensor node and another node that belongs to another network forward a data packet coming from the other side, only if both networks can obtain the higher payoffs than no cooperation scenario. The simulation results showed that the VCB can save transmission energy between 20% and 30% in a certain environment.

VII. CONCLUSIONS

In this paper, we focused on heterogeneous overlapped sensor networks that were constructed at the same area. In such a situation, it is expected that the lifetime of all networks should be extended by cooperation in multiple networks. However, since the existing methods do not consider the heterogeneity in each network, fairness in terms of lifetime improvement is required. We proposed a fair cooperative routing method with shared nodes, with the aim to achieve fair lifetime improvement in heterogeneous overlapped sensor networks. Simulation results showed that the proposed method extended the network lifetime. In particular, Pool-based cooperation achieved quite small variance of lifetime improvement, that is, it provided quite fair cooperation. As a future work, we try to implement the proposed method on an experimental system and evaluate its feasibility. Simulation results showed that the proposed method

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003062

extended the network lifetime. In particular, Pool-based cooperation achieved quite small variance of lifetime improvement, that is, it provided quite fair cooperation. As a future work, we try to implement the proposed method on an experimental system and evaluate its feasibility.

REFERENCES

1. 1J. Yick, B. Mukherjee and D. Ghosal, "Wireless sensor network survey, " Computer Networks, 52, pp. 2292–2330, April 2008.
2. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks, " IEEE Communications Magazine, Vol. 40, No. 8, pp. 102–114, August 2002.
3. I.Dietrich and F. Dressler, "On the Lifetime on Wireless Sensor Networks," ACM Transactions on Sensor Networks, Vol. 5, No. 1, Article 5, February 2009.
4. M. Perillo, Z. Cheng and W. Heinzelman, "On the problem of unbalanced load distribution in wireless sensor networks, " Proceedings of the IEEE GLOBECOM Workshops on Wireless Ad Hoc and Sensor Networks, pp. 74–79, December 2004.
5. J. Li and P. Mohapatra, "Analytical modeling and mitigation techniques for the energy hole problem in sensor networks, " Pervasive and Mobile Computing, Vol. 3, issue 3, pp. 233–254, June 2007.
6. X. Wu, G. Chen and S. Das, "Avoiding Energy Holes in Wireless Sensor Networks with No uniform Node Distribution, " IEEE Transactions on Parallel and Distributed Systems, Vol. 19, No. 5, pp. 710–720, May 2008.
7. J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," Comput. Netw., vol. 52, no. 12, pp. 2292– 2330, Aug. 2008.
8. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Commun. Mag., vol. 40, no. 8, pp. 102–114, Aug. 2002.
9. Dietrich and F. Dressler, "On the lifetime of wireless sensor networks," ACM Trans. Sensor Netw., vol. 5, no. 1, Feb. 2009, Art. no. 5.
10. M. Perillo, Z. Cheng, and W. Heinzelman, "On the problem of unbal- anced load distribution in wireless sensor networks," in Proc. IEEE GLOBECOM Workshops Wireless Ad Hoc Sensor Netw., Dec. 2004, pp. 74–79.
11. Sunar Mohammed Farook and K.NageswaraReddy , "Implementation of Intrusion Detection Systems for High Performance Computing Environment Applications ,"in IJSETR.
12. N. T. H. Phuong and H. Tuy, "A unified monotonic approach to generalized linear fractional programming," Journal of Global Optimization, vol. 26, no. 3, pp. 229–259, 2003.
13. L. P. Qian, Y. J. Zhang, and J. Huang, "Mapel: Achieving global optimality for a non-convex wireless power control problem," IEEE Transactions on Wireless Communications, vol. 8, no. 3, pp. 1553–1563, Mar 2009.
14. Safaka, M. J. Siavoshani, U. Pulleti, E. Atsan, C. Fragouli, K. Argyraki, and S. Diggavi, "Exchanging Secrets without Using Cryptography," arXiv:1105.4991 [cs, math], May 2011.
15. Safaka, C. Fragouli, K. Argyraki, and S. Diggavi, "Exchanging pairwise secrets efficiently," in 2013 Proceedings IEEE INFOCOM, Apr. 2013, pp. 2265–2273. [23] E. Atsan, I. Safaka, L. Keller, and C. Fragouli, "Low cost security for sensor networks," in 2013 International Symposium on Network Coding (NetCod), Jun. 2013, pp. 1–6.
16. K. Argyraki, S. Diggavi, M. Duarte, C. Fragouli, M. Gatzianas, and P. Kostopoulos, "Creating Secrets out of Erasures," in Proceedings of the 19th Annual International Conference on Mobile Computing & Networking. New York, NY, USA: ACM, 2013, pp. 429–440.
17. S. P. Boyd and L. Vandenberghe, Convex Optimization. Cambridge University Press, Mar. 2004.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details