World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:3, No:3, 2009

Dynamic Window Secured Implicit Geographic Forwarding Routing for Wireless Sensor Network

Z.M. Hanapi, M. Ismail, K. Jumari, and M. Mahdavi

***Abstract*—**Routing security is a major concerned in Wireless Sensor Network since a large scale of unattended nodes is deployed in ad hoc fashion with no possibility of a global addressing due to a limitation of node's memory and the node have to be self organizing when the systems require a connection with the other nodes. It becomes more challenging when the nodes have to act as the router and tightly constrained on energy and computational capabilities where any existing security mechanisms are not allowed to be fitted directly. These reasons thus increasing vulnerabilities to the network layer particularly and to the whole network, generally. In this paper, a Dynamic Window Secured Implicit Geographic Forwarding (DWSIGF) routing is presented where a dynamic time is used for collection window to collect Clear to Send (CTS) control packet in order to find an appropriate hoping node. The DWIGF is expected to minimize a chance to select an attacker as the hoping node that caused by a blackhole attack that happen because of the CTS rushing attack, which promise a good network performance with high packet delivery ratios.

***Keywords*—** sensor, security, routing, attack, random.

I. Introduction

ROUTING protocol ensures the message reaches a correct receiver in an accurate form and within a reasonable time delay. In traditional network, the nodes that do the data processing are different from the communication nodes, which responsible to relay the message to the destination. However in Wireless Sensor Network (WSN), the sensor nodes have to act in both actions. With this way, routing design becomes tricky due to limitation on nodes capabilities (i.e. easily be destroyed, exhausted of energy or power, lower bandwidth, little processing power, and limited sensing region [1,2] that can lead to a node failure. Node failure will result in inability to do its normal processing and fail to route the processing data to the destination. These limitations also cause any security mechanism developed for other networks cannot be directly applied in WSNs.

In the presence of attacker, routing or network layer becomes more critical due to the high probability that the network will drop or misdirect the packet along the way since the messages may traverse many hops before reaching the destination especially in a large scale deployment of sensor nodes [3]. Attackers then can eavesdrop [4], inject bits and replay the packets at this layer especially in wireless communication. Attackers can use many colluding nodes and the node can be more powerful than normal sensor nodes. Therefore better routing strategies and techniques should be developed to ensure the goal of routing protocol is fulfill.

The rest of the paper is organized as follows. In the next section, a general survey of routing protocols in WSN is briefly discussed and subsequently followed by a brief discussion on security issues in WSN. Then it followed with a brief review methodology specifically discussed on Implicit Geographic Forwarding (IGF) and Secured IGF. General overview of Dynamic Window Secured Implicit Geographic Forwarding (DWSIGF) is then discussed. System assumptions are briefly explained in the next section followed with detailed evaluation on DWSIGF. Finally, it wrapped with brief discussion and conclusion.

Z.M. Hanapi is with the Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor, MALAYSIA (603- 89216837; e-mail: zurina@ vlsi.eng.ukm.my).

M. Ismail is with Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor, MALAYSIA. He is now with the Department of Electrics, Electronics, and Systems Engineering (603- 89217004; fax: 603- 89254675; e-mail: mahamod@eng.ukm.my).

K. Jumari is with Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor, MALAYSIA. He is now with the Department of Electrics, Electronics, and Systems Engineering (e-mail: kbj@eng.ukm.my).

M. Mahdavi is with the Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor, MALAYSIA. (e-mail: mina@ vlsi.eng.ukm.my).

II. Background

A. Routing Protocols

Routing technique is strongly dependent on the particular application for which the WSN is used. Each application (i.e. military, health, environmental, home, etc) has different requirements on the routing strategies.

Generally, routing protocol in WSN can be classified into three different categories; flat, hierarchical, and location based routing. All nodes are typically assigned a same functionality and roles in the flat-based routing not like in hierarchical-based routing, where the nodes have different roles to play as in Low Energy Adaptive Clustering Hierarchy (LEACH) routing protocol by Heinzelman et al. [5]. On the other hand, location-based routing uses node's location for addressing (i.e. Geographic and Energy Aware Routing (GEAR) by Yu et al. [6] and IGF [7]). The position of a node can be relative or absolute to its neighbors and detected by Global Positioning System (GPS) or any other localization techniques.

In addition, routing protocol also can be categories based on how the sender finds a route to destination i.e. proactive, reactive, and hybrid routing. In proactive routing, all routes are computed before the actual communication takes place as opposed in reactive routing, where the routes are created on demands. In hybrid routing, these two approaches are integrated. Typically nodes in WSN are stationary except for few mobile nodes. Thus proactive routing is preferable.

The DWSIGF implementation is based on location-based routing since it inherits the behavior of IGF and SIGF routing protocol. It is also classified into reactive routing because it used a lazy binding approach where the forwarding node is chosen as late as possible.

B. Routing Security

In order to maintain the network availability, the network must be resilient to individual node failure. Node failure can happen because of zero power energy have by the node as mentioned by Karlof and Wagner [1] and due to attacks as discussed by Wood e al. [8]. In WSN, these two issues need serious attention in making sure successful transmission of data from sensor nodes to base station. However in this implementation, only security is taken into consideration even though there is tradeoff between the securities provided with the sensor nodes capabilities.

Routing attacks has been studied in great details by Karlof and Wagner [1], Wood et al. [8], and Hanapi et al. [3] (i.e. state corruption, wormholes attack, HELLO floods attack, blackholes attack, selectively forwading attack, Sybil attacks [9], and Denial of Service (DoS)) attack. Since DWSIGF inherits the behaviors of IGF, then few of those attacks are indirectly eliminated as discussed below.

DWSIGF keeps no routing table since the forwarding node is computed with lazy binding approach [7] only when there is a packet to send in order to avoid route to the node that is fails or node that out of area of coverage. By looking at security aspect as discussed by Wood et al. [8], this protocol is thwarted from the routing state corruption. At the same time, DWSIGF also free from the HELLO floods, wormholes, and sinkholes attack as it is based on geographic routing. Geographic routing introduces additional security concerns since it is a distance-based routing protocol where the nodes interact only with their neighbours and taking a localized independent forwarding decision based on node's physical location given by GPS or some distributed localization protocol, and need to pass certain rules defined by the protocol. It will not allow the neighbouring nodes to advertise themselves to the sender.

However, DWSIGF still vulnerable to Sybil attack [1], blackhole attack, selective forwarding attack, and DoS attack [10]. A Sybil node could appear in more than one place at once [8,9] with different set of nodes or virtual locations. By only one attacker, it can manipulate the rest of the neighour by masquerade its location and claims the other locations are also its location. Thus with IGF routing protocol for example, the sender will route to a hole when this attack happen. However, location verifications can be done on each node as suggested by [6,11] but because of memory, energy, bandwidth and computational constraints of sensor nodes make the public key encryption, digital signature impossible in WSN as discussed by Hanapi et al. [3].

Selective forwarding and blackholes attacks can be group together as discussed by Wood et al. [8] and Hanapi et al. [3]. In DWSIGF, IGF and SIGF, the attackers always try to be selected as forwarding node by trying to always be the first node reply with Clear to Send (CTS) packet. In IGF and SIGF-priority selection, if the CTS rushing attack happen, the attacker is always be selected as the participating node. As a result, this lead to zero packet delivery ratio (PDR). The DWSIGF is trying to minimize the chances of attacker selection caused by the CTS rushing attack.

III. METHOD

IGF and SIGF have been chosen as the base routing because of their stateless routing. Memory and expensive communication can be minimized without the need of routing table. Thus this approach is suitable to be applied to the limited capability of sensor node. It is also independence on any network topology or presence of the other nodes since the route is computed on demand as late as possible. In the routing perspective, it minimized a chance of a packet to be relayed to the nodes that are moved out of range, died, or in sleep state.

A. Implicit Geographic Forwarding Routing Protocol

According to Blum et al. [7], IGF routing protocol used hybrid network/Medium Access Control (MAC) protocol. It used Ready-to-Send (RTS)/CTS hand-shake of 802.11 DCF MAC protocol. The communication hand-shake is shown in Fig 1. Communication begins when network allocation vector (NAV) of *sender S* is zero after the sender detected that there is a packet to be sent. Then it carrier sense a channel for DIFS time. The sender S then broadcast an Open RTS (ORTS) if the channel is free after the DIFS. ORTS contain sender and destination locations.

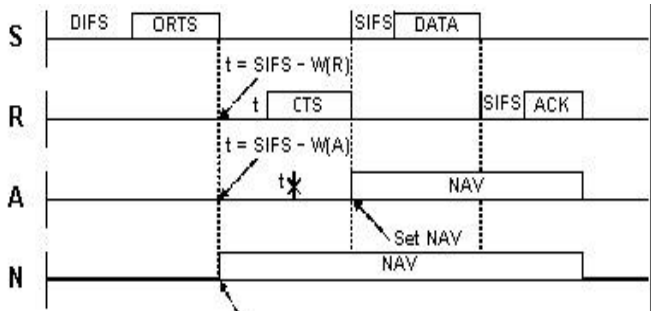

Fig. 1: IGF hand-shake timeline [7,8]

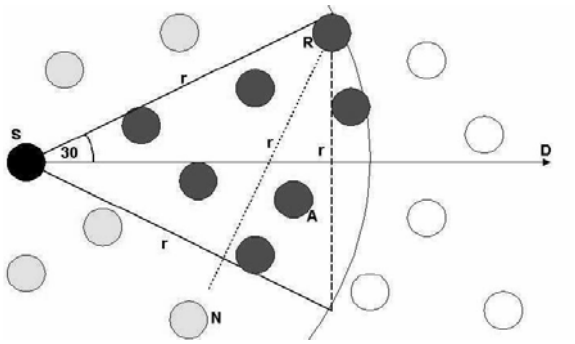

Fig. 2: Forwarding area, 60^0 sextants centered on the direct line with respect to the destination [7,8]

The *forwarding node R* is chosen at the MAC layer when *candidate nodes A* within a 60^0 sextants centered on the direct line with respect to the *destination D* replied with the CTS (contains node location) packet as shown in Fig 2. They have to set a CTS Response time [7] inversely proportional to a weighted sum of their distance from the sender, remaining energy, and at right the angles distance with respect to the destination before reply the CTS. On the expiry of the timer, they will reply the CTS packet. Other *neighbors N* that virtually overhear the CTS will cancel their CTS Response time and set their NAV based on 802.11 DCF semantics.

In IGF, only one neighbor will reply the CTS. Thus the R is confirm be selected as the forwarding nodes to relay a DATA to the destination. The communication is terminated by the acknowledgement, sent by the destination D.

B. Secured Implicit Geographic Forwarding Routing Protocol

SIGF also inherits the behaviors of IGF. It founds that without routing table, it gives zero possibility to alter and spoof routing information. However, only with a single attacker it can completely corrupt the routing for all of its neighbors. This is happen when the attacker is chosen as the forwarding node after be the first nodes reply with the CTS immediately after received the OTS in any of the hop count. Once be selected, the sender will relay the DATA to the attacker. Upon receiving the DATA, it will reply with the ACK but then can either drop or selectively forward the DATA packet to the next hop or destination.

In that case, SIGF overcomes the chances of attacked by verify all the CTSs received. In this case, all candidates within 60^0 sextants centered on the direct line to the destination will reply with the CTS but the SIGF only received any CTS that arrived within *5 ms* of sender's collection window. The candidate's locations will then be verified. However with

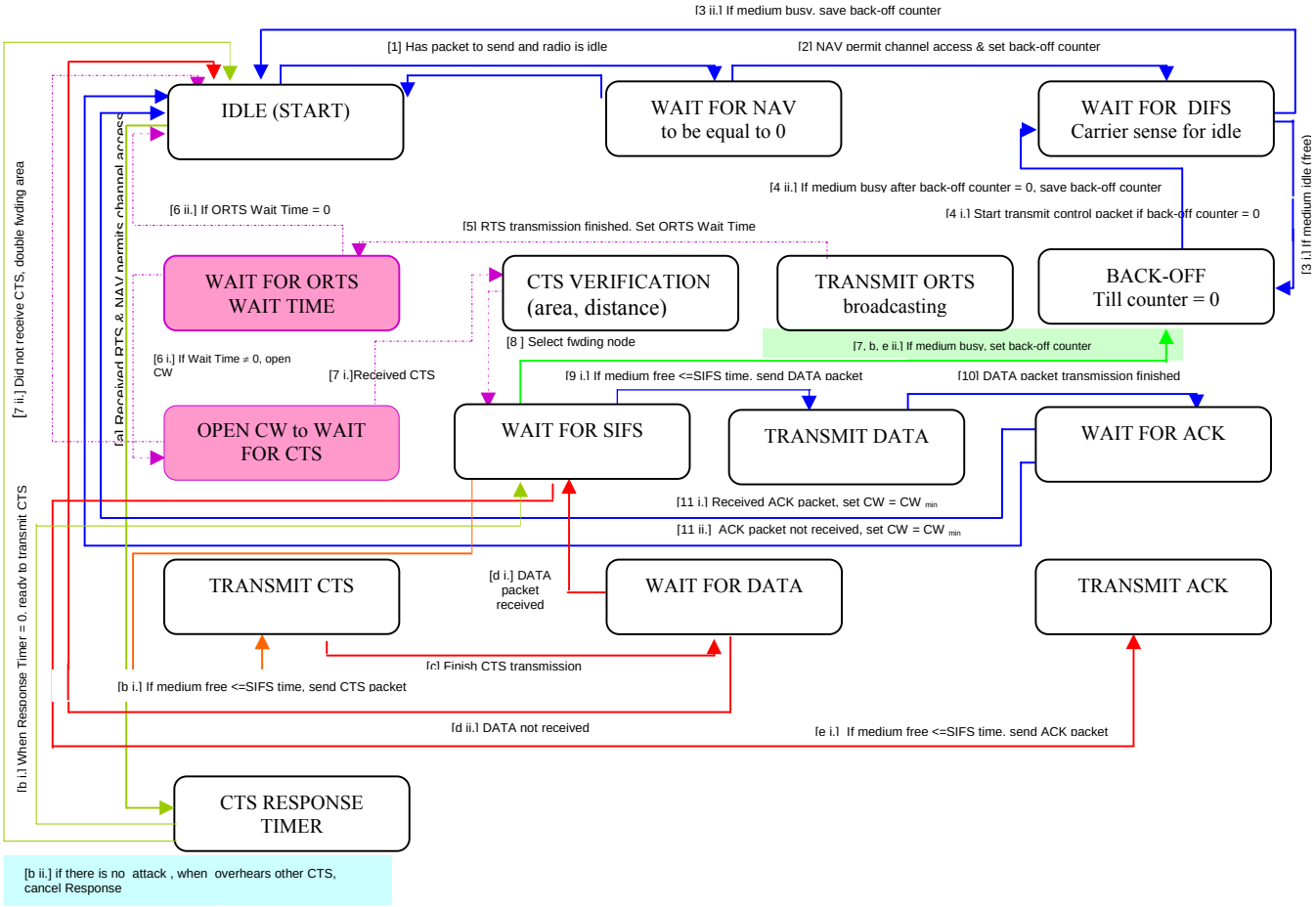

Fig. 3: State Diagram of MAC handshake for IGF, SIGF, and DWSIGF [12]

priority selection, attackers again be selected as the forwarding nodes that lead to other routing attacks as well.

IV. DWSIGF: Dynamic Window Secured IGF

DWSIGF still keeps the advantages of IGF but try to minimal a possibility of selecting attackers in SIGF. As we know, once attackers are chosen as the hop node, they can do anything to the all packets relays to them either drop it or selectively forward it. They are also able to eavesdrop the communication, modify the DATA and control packet (i.e. ACK packet), and replay the packet sent. In other words, they are now able to control the whole communication that will degrade the network performance as a whole.

Thus DWSIGF's aim is to minimize the change of attacker to take part on the communication. Unlike SIGF, random time is targeted to minimize a chance of adversaries to respond since they do not know an exact time the collection window is open. Collection windows will open to so many respondents of the CTS packet and its location and its remaining energy is verified simultaneously. Any node that gives a closed destination, good remaining energy and good history activity will be selected as the participating node.

At the same time, simultaneous verification can verify whether the nodes have duplicate location or not in order to avoid Sybil attacker as well. Once selected by the sender, they will follow the IGF semantics to relay the packet to other node towards the destination. The different between IGF, SIGF, and DWSIGF is on the collection window time as illustrated in the shaded box in Fig 3 with the method of first come first selected, fixed time, and dynamic time respectively. The fig illustrates the RTS/CTS, DATA and ACK hand-shake for IGF, SIGF, and DWSIGF in details as elaborated in section III.

V. Simulation

A. Assumption

In the implementation, communication is assumed unsecured where there will always be an attacker in the communication link between sender and receiver. There is no different between the attackers and nodes capabilities. At the same time, the nodes are remains stationary once deployed. The nodes know their own location based on the GPS reading or any other localization techniques. Furthermore, the nodes thrust their own clock, measurements and storage.

B. System Configuration

DWSIGF, SIGF and IGF are implemented using MATLAB 7.0. that follows the 802.11 MAC DCF handshaking. General system parameter is listed in Table 1.

The simulation is run within a terrain of 150 x 150 m with the number of nodes that uniformly divided into 196 cells having a communication range 40 m radius, r. Each node is placed in center using Gaussian distribution with standard deviation of 4 m. Radio bandwidth and payload size is limited to 200 kbps and 32 bytes respectively to run 100 packets of CBR streams for ten times. The result is a mean of ten simulation runs.

TABLE 1
System Parameters for Simulation

Terrain	150 x 150 meters
Number of Nodes	196
Node Placement	Grid + Ɲ(0,16) noise
Application	CBR streams
Payload Size	32 bytes
Simulation Length	100 packets, 10 runs
Radio Range	40 meters
Radio Bandwidth	200 kbps
W_P	2
W_R	1

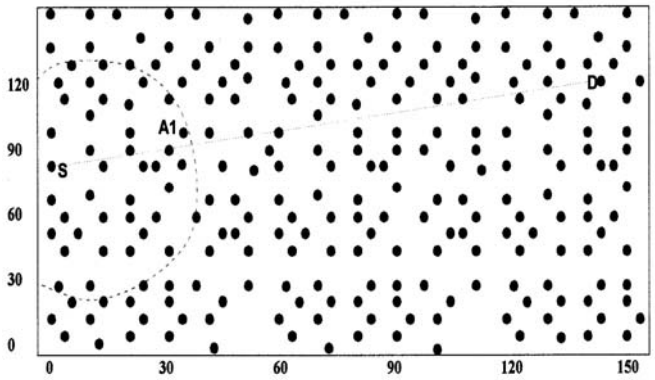

Fig. 4: Deployment of 196 nodes with sender S, destination D, and attacker A1

The simulation test point to point and many to many CBR flows. Since the result for many to many just a multiplication of point to point traffic flow, then the result shown is based on many to many traffic with 6 senders situated at the left side of the region and 2 receivers at the right of the region. The experiments evaluate the protocol under increasing traffic loads until the traffic becomes 12 packets per second. In the simulation, only one attacker is created to perform the blackhole attack caused by the CTS rushing attack. Fig 4 shows the sender S, destination D, and attacker A1 used in the experiments.

VI. Result

Simulation is done in two different scenarios; without attack and with CTS rushing attack that lead to the blackhole attack as well. Generally, all simulation results give an average of 4-6 hops count for randomly chosen 6 senders and 2 destinations.

A. Without Any Attack

Figs 5, 6, and 7 shows results without attack done on IGF, SIGF (with priority selection), and DWSIGF (with priority selection) routing protocols under increasing traffic loads with respect to PDR, end-to-end delays, and message overhead respectively. These results act as a baseline for the comparison when there is attacker performs the attacks.

Fig 5 shows IGF, SIGF, and DWSIGF have comparable delivery ratios 95-100% under light traffic load. When the

traffic starts to flow with rates 7 packets per second, each protocol start to suffer congestion. SIGF and DWSIGF degrades 0.1% and 4% respectively to IGF because of the protocols allow additional time to collect multiple CTS packet. In SIGF, fixed collection window time is used for each CBR flow however DWSIGF used dynamic window time. In the case of longer time is used for any of the communication flows, thus the number of CTS packet being collected in DWSIGF is high compared to SIGF.

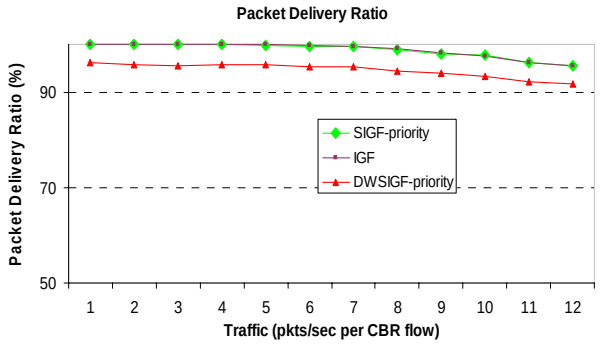

Fig. 5: Packet Delivery Ratio (PDR): without Attack

The effect of given extra time on collection window in collecting the CTS packet also increase the end to end delay of SIGF and DWSIGF with 17% and 19% respectively when compared to IGF as shown in Fig 6. This trade-of however enhances the security aspect of the protocol itself. The SIGF and DWSIGF inherits some of the general behaviors of IGF (i.e. used MAC control packets; ORTS, CTS, and ACK). Therefore, there is no big different on the communication overhead even in heavy traffic load as shown in Fig 7 except extra CTS packets are sent in SIGF and DWSIGF depending on the time allocated for the collection window with 4% and 5% increment respectively with respect to IGF.

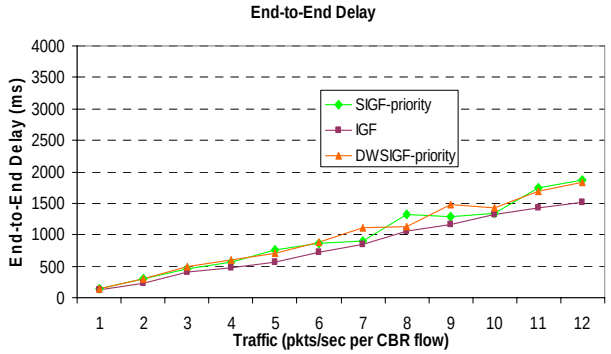

Fig. 6: End to End Delay: without Attack

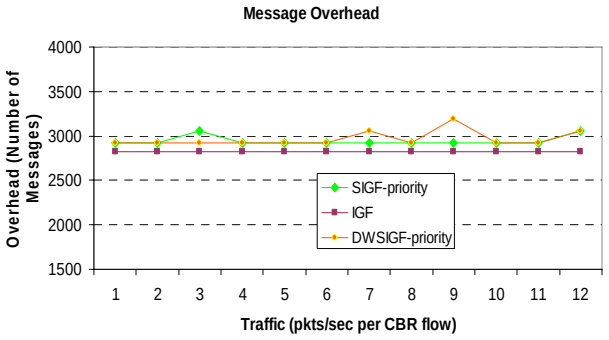

Fig. 7: Message Overhead: without Attack

In summary, DWSIGF add extra overhead compared to SIGF and IGF since dynamic collection time is used. These results acts as a baseline to investigate the protocols under blackhole attack. However, the IGF considered a perfect solution to be used when there is no attacker in the communication.

B. With Blackhole Attack

In this simulation, blackhole attack is created when the attacker A1 in Fig 4 performs the CTS rushing attack. Once being selected as the forwarding node, then it sends a virtual ACK to sender but all the packets received are actually dropped and not be relayed to the destination. As a result, the PDR becomes zero percent. The experiment with attack is evaluated with a single CBR stream in order to avoid network congestion. Since the baseline shows the network started to congest when the flow rates is 7 packets per second, thus for simplicity, existence of attacker is checked in this traffic rates.

Fig 8 shows with dynamic time allocated to collection window used in DWSIGF, the chances to select attacker as forwarding is reduced about 80%. This is because the attacker is not sure the time the collection window is close unless the attacker try to be the first node reply the CTS. In some of the cases, even the attacker try to be the first reply with the CTS, no chances for them reply the CTS because of the small time allocated to open the collection window. With the less possibility to choose the attacker thus the PDR becomes better as shown in Fig 9 with 96% PDR compared to SIGF and IGF protocol. Generally, Fig 10 shows PDR for IGF, SIGF, and DWSIGF for every traffic loads. The DWSIGF achieve mean of 90-96% PDR even there is an attacker in the communication link. However for all traffic load, IGF and SIGF-priority have a very bad performance on PDR since the attacker simply drop the entire received packet.

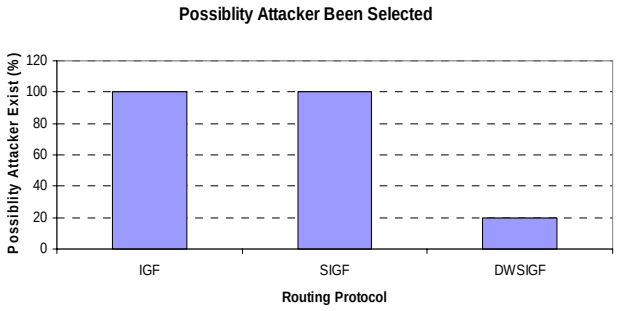

Fig. 8: Possibility of Select an Attacker

The DWSIGF still can provide a good PDR (mean of 90-95 %) even the neighbors performing the blackhole attack due to less possibility to selects the attacker as the forwarding node as compared to SIGF and IGF.

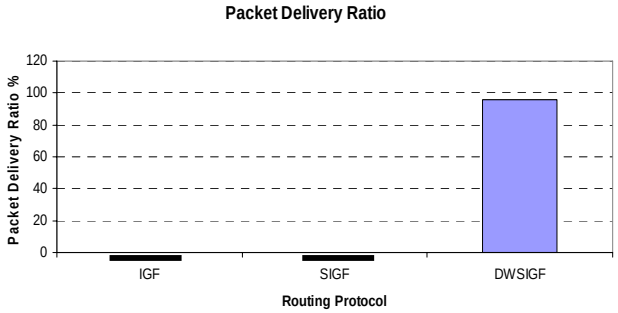

Fig. 9: Packet Delivery Ratio on 7 packets/sec per CBR flows: Blackhole Attack

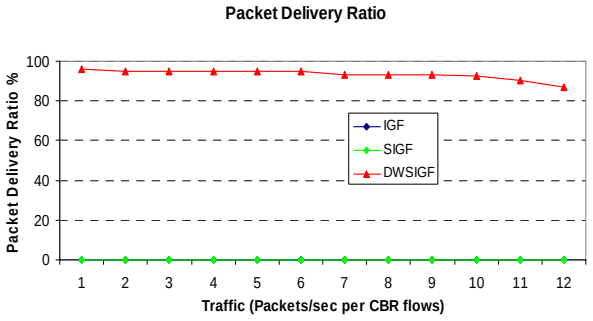

Fig. 10: Packet Delivery Ratio: Blackhole Attack

C. Discussion

Our simple approach is promising a minimal risk in selecting attacker as the forwarding node caused by the CTS rushing attack. Thus reduce the chance of having the blackhole attack and increase the network performance as a whole. Since our routing protocol inherits the behavior of IGF strategies, then the wormholes, HELLO flood, sinkholes attacks, and spoofing and altering of routing table are also not possible even without any security techniques and mechanisms applied on it. Each node will make an independent decision in choosing its next hop based on node's physical location given by GPS or any other localization techniques. This approach also limits the impact of attacks to just a local neighbourhood because the participating node is fully independent and dynamically chosen and as late as possible. Lastly with geographic routing properties, it is also resistant to insiders and outsiders attackers since it do not trust its neighbouring nodes.

However, our protocol still vulnerable to selective forwarding, Sybil, and DoS attacks. The adversaries node always competes to send the respond control packet as early as possible in order to make sure always be selected as a next hop. Since our protocol requires next hop's candidate to pass certain criteria or rules, then there is no possibility for the attackers to send wrong information to the sender and claims it is a right next hop to be chosen. We will further discuss our routing strategies and defense methods in our next paper.

VII. Conclusion

In this paper, the DWSIGF, the dynamic window stateless routing protocol that resilience to blackhole attack caused by the CTS rushing attack is presented. The simulation evaluated the test without the attack and with the blackhole attack. Even without inserting any security mechanism inside the routing protocol, the DWSIGF still promise a good defense against blackhole attack with better performance on PDR. However, IGF still be a good solution when there is no attack in the network. Future work is to developed suitable defense against selective forwarding, Sybil, and DoS attacks to suit with our routing algorithm.

Acknowledgment

We would like to thank the reviewers for their comments. This work was supported by research grant UKM-OUP-NBT-29-153/2008.

References

[1] Karlof, C. and Wagner, D., "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", *Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols*, 2003, 1(2003), 293-315.

[2] Yick, J, Mukherjee, and Ghosal, D., "Wireless Sensor Network Survey", *Journal of Elsevier: Computer Network*, 2008 52(12):2292-2330.

[3] Hanapi Z.M., Ismail M., Jumari K., and Mirvaziri H., "Analysis of Routing Attacks in Wireless Sensor Network", *In Proceedings of International Cryptology Workshop and Conference (Cryptology2008)*, 2008, ISBN 978-983-4069, pp. 202-214.

[4] Kuo, C., Luk, M., Negi, R., and Perrig, A., "Message-In-A-Bottle: User Friendly and Secure Key Deployment for Sensor Nodes", *In Proceedings of International Conference of Sensor System (SenSys2007)*, 2007, ACM-159593-763-6/07/0011.

[5] Heinzelman, W.R., Chandrakasan, A., and Balakrishnan, "Energy-efficient Communication Protocol For Wireless Sensor Networks", 2000. pp. 3005-3014.

[6] Wood, A.D. and Stankovic, J., "Denial of Service in Sensor Networks", *IEEE Computer*, 0018-9162/02, pp.54-62.

[7] Blum, B., He, T., Son, S, and Stankovic, J., "IGF: A State-Free Robust Communication Protocol For Wireless Sensor Network", *Technical Report CS-2003-11*, University of Virginia, 2003.

[8] Newsome, J., Shi, E., Song, D., and Perrig, A., "The Sybil Attacks In Sensor Networks: Analysis and Defense", *In Proceedings of Third International Symposium on Information Processing in Sensor Networks*, ACM 1-58113-846-6/04/0004, 2004.

[9] Wood, A.D., Lei, F., Stankovic, J., and Tian, H., "SIGF: A Family of Configurable, Secure Routing protocols for Wireless Sensor Networks", *SASN2006, ACM* 1-59593-554-1/060010, *2006*, pp. 35-48.
[10] Wood, A.D. and Stankovic, J., "Denial of Service in Sensor Networks", *IEEE Computer*, 0018-9162/02, pp.54-62.
[11] Abu G.N., Kang K., and Liu K., "Towards Resilient Geographic Routing in WSNs", *In Proceedings of Q2SWinet05,* ACM 1-59593-241-0, 2005, pp. 71-78.
[12] Hanapi Z.M., Ismail M., Jumari K., and Mirvaziri H., "A Taxanomy of Routing Attacks in Geographic Routing in Wireless Sensor Network", *In Proceedings of 1st Engineering Postgraduate Conference (EPC2008): Innovation through Engineering, 2008.*

Hanapi Z.M. received her first degree in BSc. Computer and Electronic System from the University of Strathclyde, Glasgow, UK in 1999. The author then received her master degree in MSc. Computer and Communication System Engineering from Universiti Putra Malaysia (UPM), Selangor, Malaysia in 2004.

Currently she is a Ph.D student at a Department of Electric, Electronic, and System Engineering, Faculty of Engineering and Built Environment, Universiti Kebangsaan Malaysia (UKM). The selected paper that she had published are Hanapi Z.M., Ismail M., Jumari K., and Mirvaziri H., "Analysis of Routing Attacks in Wireless Sensor Network", *In Proceedings of International Cryptology Workshop and Conference (Cryptology2008)*, 2008, ISBN 978-983-4069, pp. 202-214, Hanapi Z.M., Ismail M., Jumari K., and Mirvaziri H., "A Taxanomy of Routing Attacks in Geographic Routing in Wireless Sensor Network", *In Proceedings of 1st Engineering Postgraduate Conference (EPC2008): Innovation through Engineering*, 2008 and Mirvaziri, H., Jumari, K. and Ismail, M., and Hanapi, Z.M., "Collision Free HASH Function Based on Miyaguchi-Preenel and Enhanced Merkle-Damgard Scheme", IEEE *5th Student Conference on Research and Development*, 2007. Her current research interests are on routing security, wireless sensor network, and distributed computing.

Ms. Zurina is a member on Malaysian Security Committee Research (MSCR).

Ismail, M. (M'94– EC'04– SM'06). This author became a Member (M) of IEEE in 1994, Executive Committee in 2004, and Senior Member in 2006. The author received the BSc. degree in Electrical and Electronics from the University of Strathclyde, Glasgow, UK in 1985. The author then received his MSc. degree in Communication Engineering and Digital Electronics from the UMIST, Machester, UK in 1987, and the Ph.D. from University of Bradford, U.K. in 1996.

Currently he is a Professor in the Department of Electrical, Electronics, and System Engineering, Faculty of Engineering and Built Environment, UKM. He is also a Deputy Director (Research) for the Centre for Information and Communication Technology, UKM, and a Senior Fellow for Institute of Space Science, UKM. The selected paper that he had published are Chee K.N., Noordin, N.K. ,Khatun, S., Ali, B.M., Sudhanshu, S.J., and Ismail, M., "Directional Diversity of Smart Antenna in LAS CDMA Systems", *Journal of Wireless Personal Communications, , Springer Netherlands*, August 2008, Vol. 46, No. 3, pp. 305-316 (ISI & SCOPUS), K. Singh, M. Ismail, K. Jumari, M. Abdullah, and K. Mat, "Development of Universal Intelligent Positioning System Techniques in Universal Mobile Telecommunications System Networks", *Journal of Applied Sciences, Asian Network for Scientific Information, Pakistan*, July 2008, Vol. 8, No. 13, pp. 2412-2419, ISSN: 1812-5654 (ISI), and Yusof, A.L., Ismail, M., and Misran, N., "A New Signaling Protocol For Seamless Roaming In Heterogeneous Wireless Systems", *Ubiquitous Computing and Communication Journal (UbiCC)*, April 2008, pp. 3(2):1-8., ISSN 1992-8424. His current research interests are mobile communication and wireless networking (radio resource management).

Prof. Dr. Ismail is a Technical Expert Panel on ICT Sector, RMK9 e-Science Fund, Ministry of Science, Technology and Innovation (MOSTI)/MDeC, a member for Malaysian Research Newtwok (MyREN), Malaysia, and IPv6 Study Group, Asian Pasific Advanced Network (APAN) Malaysia.

Jumari, K. This author received the BSc. (Hons) degree in Physics from the UKM, Malaysia in 1976. The author then received his MSc. degree in Instrument Design from the University of Aberdeen, UK in 1978, and the Ph.D. from University of Kent, U.K. in 1985.

Currently he is a Professor in the Department of Electrical, Electronics, and System Engineering, Faculty of Engineering and Built Environment, UKM. He is also an Associated Fellow at Institut Sains Angkasa (ANGKASA), UKM, and a leader of Computer & Network Security Research Group at the Department of Electrical, Electronics, and System Engineering, Faculty of Engineering and Built Environment, UKM. The selected paper that he had published are Alrashdan, M., Ismail, M., and Jumari, K., "A Study on Effective Transfer Rate Over Smart Hierarchical Mobile IPv6 (SHMIPv6)", *International Journal of Computer Science and Network Security* , 2007, Vol. 7 No. 5, pp. 235-239., Ibrahim, A.H., Ismail, M., Jumari, K., and Salleh, A, "SOM and Cost Optimization Tools for ITLMS via LOS Link System", *European Journal of Scientific Research*, Vol. 16, No. 4 , 2007, pp. 524-530., and Angkat H., Rahmat R.A., Jumari K., Hassan A., and Basri H, "Smart Traffic Surveillance System", *International Journal of Engineering Science & Technology*, 2006, Vol. 5, No. 1, pp. 41-51. His current research interests are on Computer Network Security, Image Processing, and Multimedia Communication.

Prof. Dr. Jumari was the Head of the Department of Electrical, Electronics, and System Engineering, Faculty of Engineering from November 1985 to March 1990, the Deputy Dean of Engineering Faculty, UKM from November 1991 to May 1995, and the Director of Computer Center, UKM from May 1995 to May 2006.

Mahdavi, M. received her BEng. degree in Electronic Engineering from University of Ferdowsi , Mashhad , Iran in 1992. This author then received her MEng. degree in Communication and Computer Engineering from UKM, Selangor, Malaysia in 2006.

Currently she is a PhD candidate in the Department of Electrical, Electronics and System Engineering, Faculty of Engineering and Built Environment, UKM . Her current research interests include energy efficiency, energy efficient node scheduling, coverage and connectivity in wireless sensor networks.