http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 9 (3): 545-552, 2010
ISSN 1812-5638

The Impact of Window's Size in DWSIGF Routing Protocol

Z.M. Hanapi, M. Ismail, K. Jumari, M. Mahdavi and H. Mirvaziri
Department of Electrical, Electronics and Systems Engineering,
Faculty of Engineering and Built Environment, Universiti Kebangsaan Malaysia, Selangor, Malaysia

Abstract: In this study, different collection window's size is been analyzed to investigate the impact on network performance: packet delivery ratio, message overhead and end to end delay on the Dynamic Window Secured Implicit Geographic Forwarding (DWIGF) routing protocol where this protocol is based on a dynamic collection window approached. Its method on using dynamic window's size has minimized the probability of selecting attackers and guaranteed high packet delivery ratios when there is a blackhole attack in the communication link. The DWSIGF is then compared with the best chosen window's size to analyze the network performance with and without attacker in the communication line, respectively. The DWIGF is able to minimize a Clear To Send (CTS) rushing attack that leads to a blackhole and selectively forwarding attack with a guaranteed of high packet delivery ratios where a selection of a failed node and an attacker is minimized, respectively. As a result, this routing protocol is promising a dynamic and secured communication without inserting any existing security mechanism inside.

Key words: Dynamic window, secured routing, sensor network, routing attacks, lazy binding, geographic routing

INTRODUCTION

Wireless Sensor Network (WSN) consists of large numbers of low-power and low cost nodes deployed more likely at the fixed locations. General activity of these sensor nodes is to monitor and protect the environment especially in the area that cannot be attended by the human but need special attention, i.e., military, environmental, safety critical and domestic infrastructures and resources.

Sensor node collects and analyzes low level data as well as behaves as a router but with limited capabilities as discussed by Karlof and Wagner (2003) and Yick and Ghosal (2008) (i.e., easily be destroyed, exhausted of energy or power, lower bandwidth, little processing power and limited sensing region that can cause a node failure (Wood and Stankovic, 2002) . The node failure can affect the whole network performance since, the targeted data cannot be processed and gathered at the appropriate time and lead to a network down since, the nodes could not route the data to the receiver or the base station.

Moreover, the node failure also can takes place when there is an attacker during the communication (Wood *et al*., 2006). According to Hanapi *et al*. (2008) in the presence of attacker, the 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 reach the destination especially in a large scale deployment of sensor nodes. Attackers then can eavesdrop as mentioned by Kuo *et al*. (2007) and Hanapi *et al*. (2009), inject bits and replay the packets at this layer especially in a wireless communication (Yick and Ghosal, 2008). Therefore, the confidentiality and integrity of the data being transmitted is reduced dramatically (Qian *et al*., 2007).

Furthermore, the attackers also can use many colluding nodes or more powerful devices (i.e., laptop class attacker) to be more powerful than normal sensor nodes where the attacks can be performed more easily. Thus, in order to maintain the network availability and successful transmission in WSN, the network must be resilient to individual node failure.

Wood *et al*. (2006) have discussed that zero power energy and attacks are the serious issues that caused the node failure. However in this study, only security issue is taken into consideration for the DWSIGF implementation because in WSN, any existing security mechanism cannot be directly fitted or applied due to limited capabilities of sensor node itself as discussed by Wood and Stankovic (2002). In the case of encryption and decryption mechanism, its implementation requires more memory and

Corresponding Author: Z.M. Hanapi, Department of Electrical, Electronics and Systems Engineering, Faculty of Engineering and Built Environment, University Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia Tel: +60389216837 Fax: +60389216146

powerful processing power that cannot be adopted by the sensor node. Thus, improvement of routing strategies can be one of solution to provide the secured routing for the WSN.

In DWSIGF, few of routing attacks that has been studied by Karlof and Wagner (2003), Wood *et al*. (2006) and Hanapi *et al*. (2008) (i.e., state corruption, wormholes attack, HELLO floods attack, blackholes attack, selectively forwarding attack, Sybil attacks and Denial of Service (DoS) attacks as mentioned by Blum *et al*. (2003)) are indirectly eliminated because our protocol inherits the behaviors of Implicit Geographic Forwarding (IGF). The DWSIGF also keeps no routing table since, the forwarding node is computed with lazy binding approach as discussed by Wood and Stankovic (2002) where the hop node is calculated as late as possible when there is only a packet to send. As a consequence, it is protected from the routing state corruption while minimize the use of energy and memory (Wood *et al*., 2006). At the same time, DWSIGF also free from the HELLO floods, wormholes and sinkholes attack as it is based on geographic routing (Wood *et al*., 2006). Geographic routing introduces additional security concerns since, it is a distance-based routing protocol where the nodes interact only with their neighbors and taking a localized independent forwarding decision based on node's physical location given by GPS or some distributed localization protocol and certain rules defined by the protocol. It will not allow the neighboring nodes to advertise themselves to the sender.

Even though few routing attacks can be eliminated because of the routing strategies used by IGF routing protocol, however DWSIGF still vulnerable to Sybil attack (Abu *et al*., 2005), blackhole attack, selective forwarding attack and DoS attack. According to Wood *et al*. (2006) the Sybil node could appear in more than one place at once with different set of nodes or virtual locations. Location verifications can be done on each node as suggested by Wood and Stankovic (2002) and Abu *et al*. (2005) 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*. (2008)

On the other hand, selective forwarding and blackholes attacks can be grouped together based on Hanapi *et al*. (2008). In DWSIGF, IGF and Secured Implicit Geographic Forwarding (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, the attacker is always being selected as the participating node because it performs the CTS rushing attack. Thus, lead to zero packet delivery ratio (PDR). The DWSIGF is then take a challenge to minimize the chances of performing the CTS rushing attack and have minimal chances of selecting the attacker as the participating node. Even though DWSIGF improve on security features, the energy consumption still minimal as claimed by Newsome *et al*. (2004) and Shi *et al*. (2006) because of multi hop routing technique.

BACKGROUND

The DWSIGF inherits the approach of stateless routing used by SIGF as discussed in details in Hanapi *et al*. (2009) since, memory and expensive communication can be minimized without the need of routing table. Moreover, the lazy binding technique used also make the DWSIGF protocol independence on any network topology or presence of the other nodes since, the route is computed dynamically on demand and as late as possible. In the routing perspective, this approach minimized the used of energy and promise fault tolerance because the chanced of a packet to be relayed to the nodes that are moved out of range, died, or in sleep state is minimized (He *et al*., 2007; Akyildiz *et al*., 2002).

On the other hand, SIGF routing approach is based on the IGF routing protocol technique with hybrid network/Medium Access Control (MAC) protocol in hand. It used Ready-to-Send (RTS)/Clear-to-Send (CTS) hand-shake of 802.11 distributed coordination function (DCF) MAC protocol to avoid hidden and exposed terminal problems (Huei and Rubin, 2003) in wireless communication as the communication handshake is shown in Fig. 1 where it 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 carries sense a channel for DCF Inter-Frame Spacing (DIFS) time. The S then broadcast an Open RTS (ORTS) containing location of S and D if the channel is free after the DIFS time.

A forwarding node R is chosen when all candidate nodes A within 60° sextants centered on the direct line with respect to the destination D replied with the CTS

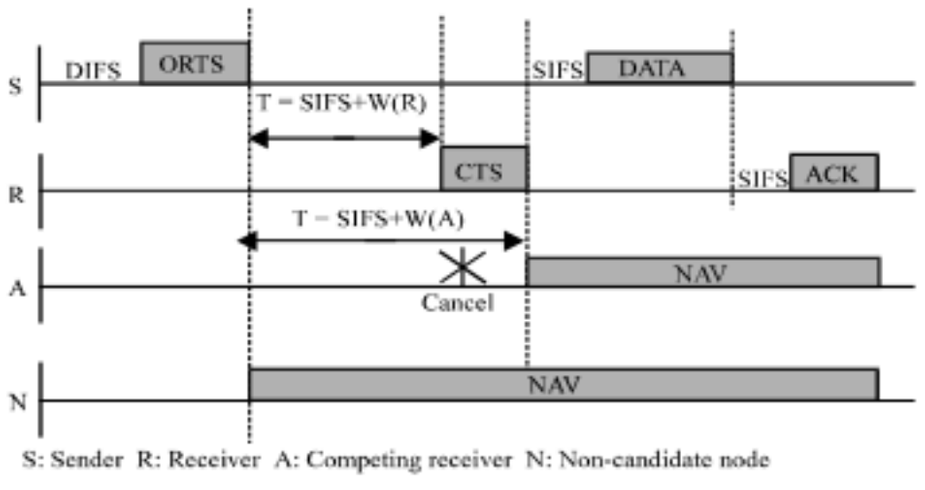

Fig. 1: IGF hand-shake timeline (Blum *et al*., 2003; He *et al*., 2007)

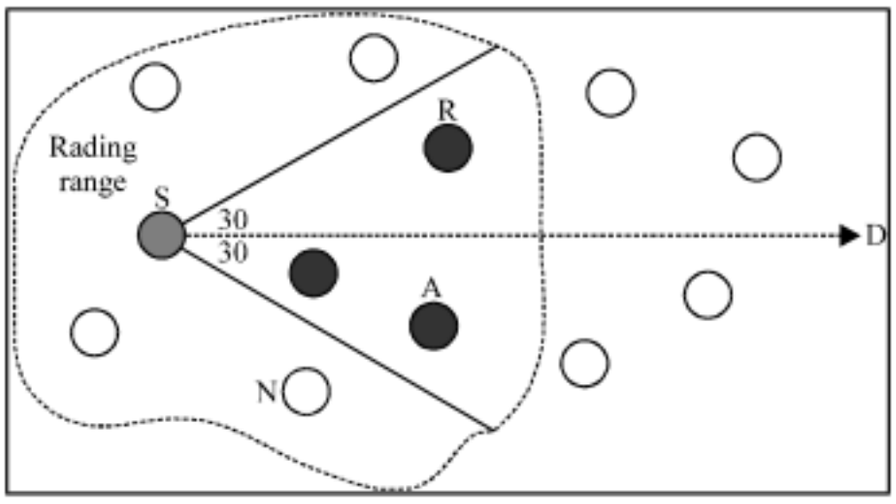

Fig. 2: Forwarding area, 60° sextants centered on the direct line with respect to the destination (Blum *et al*., 2003; He *et al*., 2007)

packet as shown in Fig. 2. The CTS packet contains a location of candidate nodes. All the candidate nodes have to set a CTS Response time (i.e., W(R) and W(S) in Fig.1) 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 with the CTS (Wood *et al*., 2006; Blum *et al*., 2003). On the expiry of the timer, they will reply with the CTS packet. Based on IGF, other neighbors N that virtually overhear the CTS packet being sent will cancel their CTS Response time and set their NAV based on IEEE 802.11 DCF semantics since, only one neighbor with minimal CTS Response time is allowed to reply the CTS packet.

As shown in Fig. 2, the R is selected as the forwarding or hop node to relay a DATA to the destination. These steps keep on going in multi hop communication until the destination D send an acknowledgment to the sender.

The SIGF protocol inherits the main behaviors of IGF with major focus on routing security (Wood *et al*., 2006). It founds that, without the routing table in IGF, it gives zero possibility to alter and spoof the routing information. However, with only a single attacker, IGF can completely corrupt the routing all of its neighbors when the attacker is chosen as the hop node. After the attacker being the first node reply with the CTS packet, it is confirmed be the next hop node. The attacker normally can break the routing rule where in this case it immediately respond with the CTS packet after received the ORTS by ignored the CTS Response time calculation. Once be selected, the sender will relay the DATA to him. Upon receiving the DATA, it will reply with the ACK but can either drop, selectively forward the DATA packet to the next hop or destination or any other illegal actions like modify or replay the DATA packets.

In order to minimize the chance of selecting the attacker as the hop node, SIGF verify all the CTSs received to authenticate hop node. All candidates within 60° sextants centered on the direct line to the destination will reply with the CTS packet within 5 m sec of sender's collection window unlike in IGF where the collection window is closed when one CTS packet is received. The candidate's locations will then be verified. However, with priority selection, attackers again be selected as the forwarding nodes.

METHODS

The DWSIGF still keeps the advantages of IGF and SIGF but with smallest possibility of selecting attackers in its communication in order to improve the network performance (Hanapi *et al*., 2009). As discussed before, once attackers are chosen as the forwarding node, they are now able to have control over the communication (i.e., drops all the packets or selectively forward the packet received, modify DATA and any control, eavesdrops the communication and replayed the packet sent). As a consequence, the network performance will degrade as a whole when the attacker is chosen as the participating node during the transmission.

Unlike SIGF, dynamic time is used for the collection window in order to minimize the chances of adversaries to take part as the hop node since, they do not know an exact duration time of the collection window. The DWSIGF will open to so many respondents to send the CTS packet and once receive it, verification of location and remaining energy of CTS's sender is done concurrently. 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 validate whether the nodes have duplicate location or not in order to avoid Sybil attacker as well. Once it is selected by the sender, the communication continues with the IGF semantics to relay the packet to other node towards the destination. The difference between IGF, SIGF and DWSIGF is on the collection window time with the method: first come first be selected, fixed time and dynamic time, respectively.

SIMULATION

Assumption: Communication is assumed unsecured in this simulation where there will always be an attacker in the communication link between sender and receiver that able to drop or modify any packet received. The nodes capabilities are also assumed similar as the attacker. At the same time, the nodes are remains stationary once deployed. Lastly, the nodes are assumed know their own location based on the GPS reading or any other localization techniques.

System configuration: DWSIGF, SIGF and IGF protocols are implemented using MATLAB 7.0 and based on the 802.11 MAC DCF handshaking.

The simulation is run within an area of 150×150 m with the number of nodes that uniformly divided into 196 cells having a communication range 40 m radius as depicted in Fig. 3. Each node location is placed within the center of grid and uniformly distributed using Gaussian distribution with standard deviation 4 m. Radio bandwidth and payload size is limited to 200 kbps and 32 bytes, respectively to run 100 packets of CBR streams for 10 times for each traffic. The value of W_P and W_R (Blum *et al*., 2003; He *et al*., 2007) is 2 and 1, respectively. The result is a mean of hundreds simulation runs.

The simulation involved point to point and many to many CBR flows. Since, the result for many to many is just a multiplication of point to point traffic flow, then the result shown is based on many to many traffic with six senders situated at the left side of the region and two receivers at the right of the region for the simulation without attack. However, with the blackhole attack simulation, only one sender, one destination is used to avoid network congestion as shown in Fig. 3.

The experiments for without attack and blackhole attack evaluate the three main protocols (i.e., IGF, SIGF and DWSIGF) under increasing traffic loads until the traffic becomes 10 packets sec^{-1}. In the simulation, SIGF and DWSIGF are evaluated thoroughly with priority and random selection of the node that sent the CTS. Priority selection is based on selecting the node that sent the first CTS to the sender whereby random selection is randomly select any node that sent the CTS.

Moreover, SIGF is then being investigated thoroughly with different collection windows ranging from 1 msec up to 9 msec to observe the affect of network performance on different collection windows time. The evaluation is also to examine a better time can be used for the collection window in SIGF as before in Wood *et al*. (2006) just used 5 m sec for the SIGF collection window. Apart from it, dynamic time for DWSIGF also changed to 0-10 msce instead of 0-5 m sec used in Hanapi *et al*. (2009).

The simulation on attack only involved one attacker, A1 to perform the blackhole attacks caused by the CTS rushing attack as shown in Fig. 3.

RESULTS

The simulation is first done on different value of time used in SIGF's collection window. In this study, the collection windows time is investigated only on SIGF with priority selection since, IGF's collection window is closed immediately once received the CTS reply from the neighbor whereby for DWSIGF, the time used to open the collection window is dynamic. In the next study through analysis will be done on SIGF with random selection. The chosen best time with better network performance will be used for the next analysis to evaluate IGF, SIGF and DWSIGF in two main different scenarios: without attack and with blackhole attack.

Collection window's time: Figure 4-6 show a network performance on Packet Delivery Ratio (PDR), message overhead and end to end delay of SIGF with different collection time. These results act as a baseline for the next evaluation on investigating a performance of DWSIGF over SIGF and IGF under attack and without attack.

Figure 4 shows SIGF with different collection windows time have comparable delivery ratios 100% under light traffic load. When the traffic starts to flow with rates 5 packets sec^{-1}, each protocol start to suffer congestion. There is no much different on the performance of PDR of each time over different traffic load, however, the best time for this analysis is when

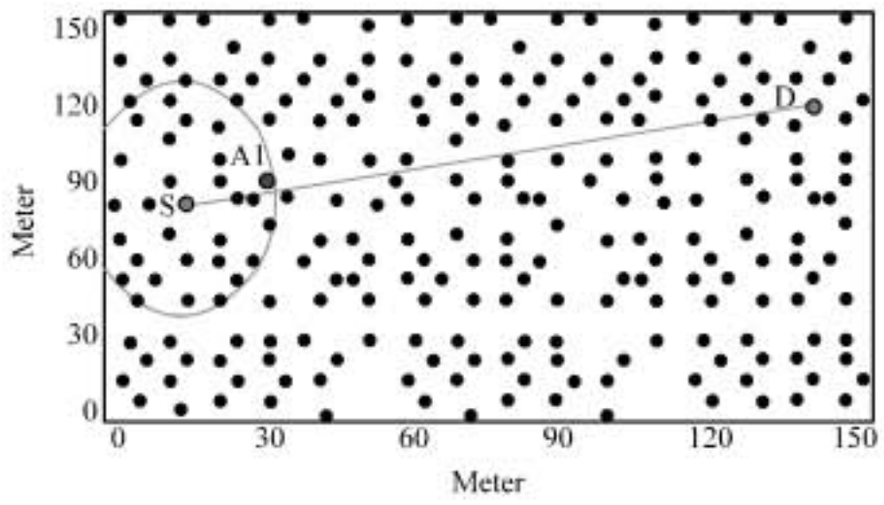

Fig. 3: Deployment of 196 nodes with sender S, destination D and attacker A1 in the area of 150×150 m

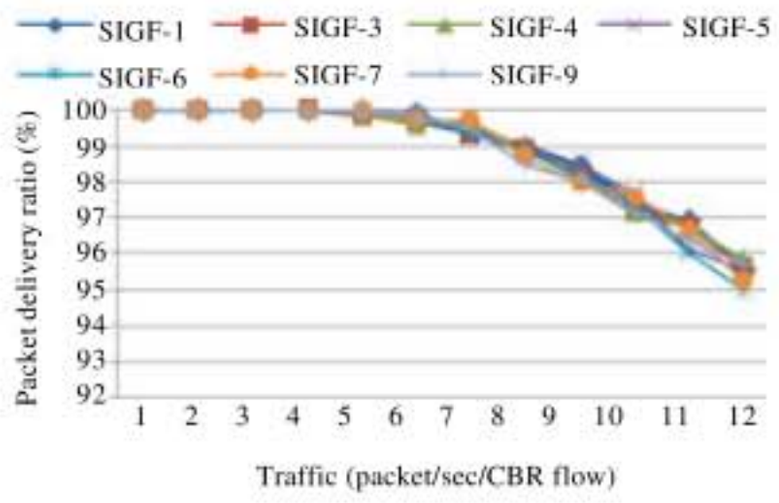

Fig. 4: Packet delivery ratio with different collection window's time

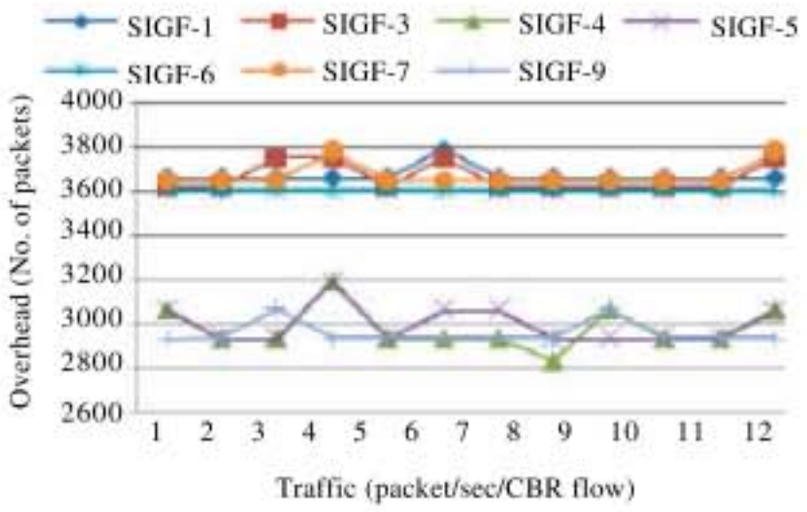

Fig. 5: Message overhead with different collection window's time

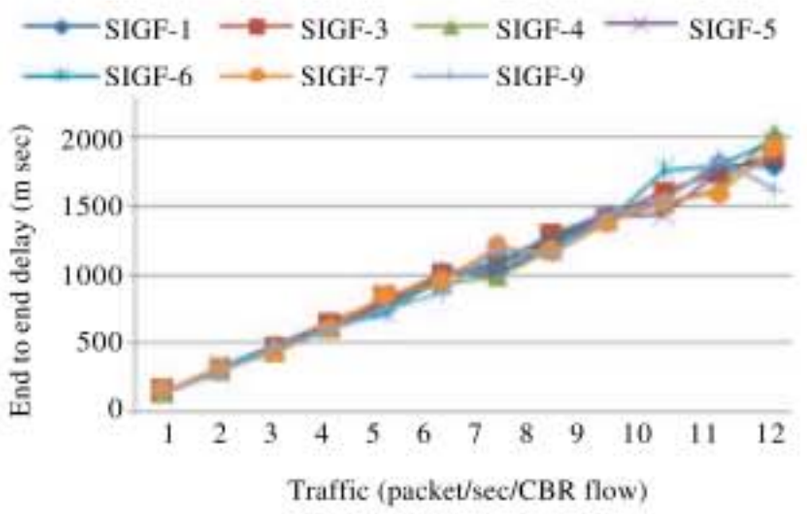

Fig. 6: End to end delay ratio with different collection window's time

time is 1, 4 and 5 m sce with SIGF-1 performs 0.056 and 0.061% better than SIGF-4 and SIGF-5, respectively.

All the experimented SIGF with different collection window's time used the same control packets (i.e., used MAC control packets; ORTS, CTS and ACK). However, as shown in Fig. 5, SIGF-9, SIGF-4 and SIGF-5 have less overhead as compared to the other evaluated SIGF with SIGF-9 performs better than SIGF-4 and SIGF-5 with less 0.73 and 1.37% overhead, respectively. The great different between the other time is because the time given to open the collection time is not enough to collect the CTS packet. Thus, requires retransmission of control packets to reinitiate the communication when not enough CTS collected during the open time of collection window.

In SIGF, fixed collection window time is used for each CBR flows. In the case of longer time to open collection window, thus the number of CTS packet being collected in is high. However in SIGF-9, the effect of given extra time on collection window in collecting the CTS packet have a better end to end delay of SIGF as compared to middle value of time as depicted in Fig. 6 with 0.37 and 1.06% less with respect to SIGF-4 and SIGF-5. This is because 9 m sec is considered enough to collect the entire CTS packet within the 60° region towards the destination.

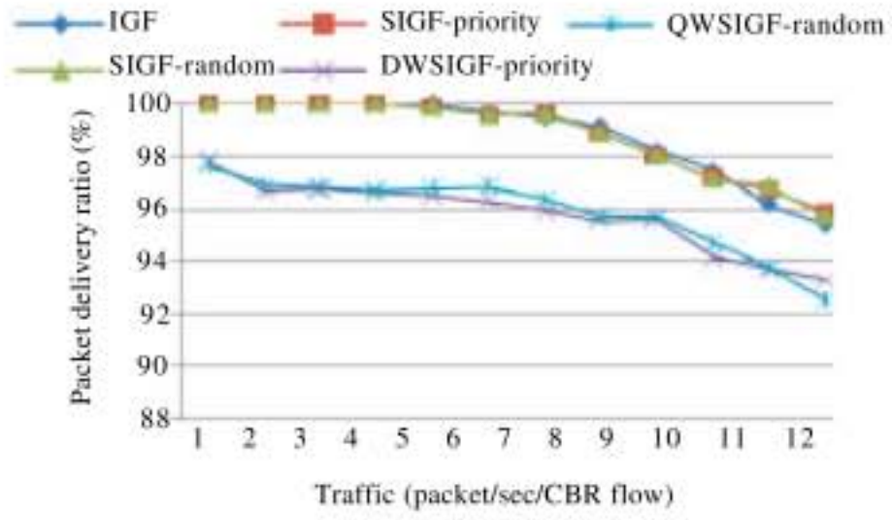

Fig. 7: Packet delivery ratio without attack

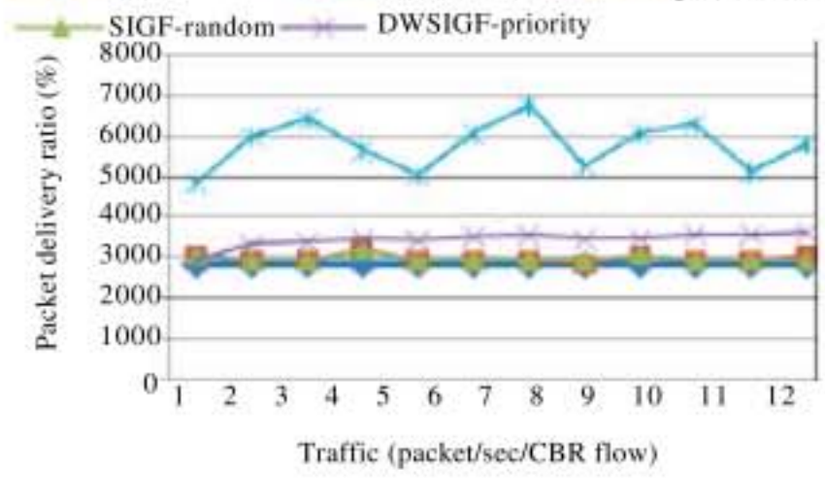

Fig. 8: Message overhead without attack

Generally from the analysis been done, SIGF-4 and SIGF-5 have better performance on PDR, message overhead and end to end delay as contrasted to SIGF-1 and SIGF-9 since, in each evaluation, these times performs better evaluation. However, when compared to 5 msec, collection time of 4 msec is much better with 0.05% better on PDR, 0.64% less on message overhead and 0.32% less on end to end delay. Thus, the best value suited in SIGF collection window's time is when time equals to 4 m sec. For the next analysis for SIGF, 4 m sec will be used for its collection window's time.

Without attack: Figure 7-9 show a performance on PDR, message overhead and end to end delay of DWSIGF, SIGF and IGF routing protocols without involving any attackers in the communication link between sender and destination.

Figure 7 shows IGF, SIGF-priority and SIGF-random have comparable delivery ratios 99-100% and DWSIGF-priority and DWSIGF-random have PDR about 95-98% under light traffic load. When the traffic starts to flow with rates 6 packets sec^{-1}, each protocol start to suffer congestion. SIGF-priority, SIGF-random, DWSIGF-priority and DWSIGF-random degrades 0.02, 0.01, 3.1 and 3%, respectively to IGF because of the protocols allow additional time to collect multiple CTS packet. It becomes

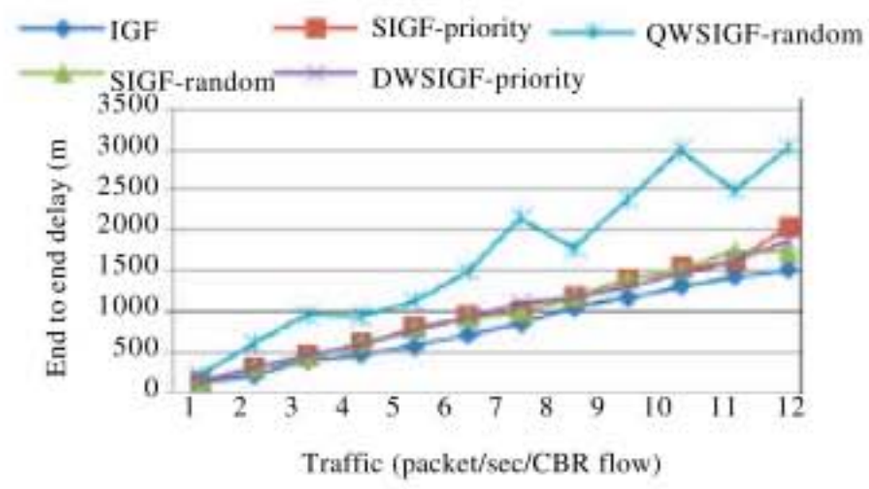

Fig. 9: End to end delay without attack

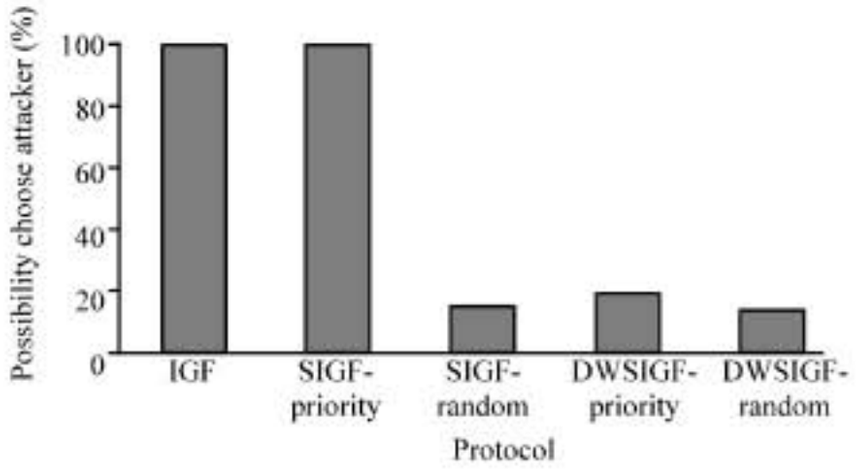

Fig. 10: Possibility of selecting attacker as forwarding node

more congested with DWSIGF since, the number of CTS packets collected is uncertain especially when longer collection windows time allocated for the transmission.

No great different on the communication overhead even in heavy traffic load as shown in Fig. 8 as the SIGF and DWSIGF used the same control packets of IGF during the communication. In the case of extra CTS packets are sent in SIGF-priority, SIGF-random and DWSIGF-priority depending on the time allocated for the collection window of 4 msec for SIGF and 0-10 msec for DWSIGF, performance on overhead degrades with 5, 5.5 and 20%, respectively with respect to IGF. In DWSIGF-random, the communication overhead almost double with respect to the IGF routing protocol because of retransmission of control packets to reinitiate the communication. This is due to not enough CTS collected during the open time of collection window and also multiples CTS packet collected during longer time of opening the collection window.

In SIGF, fixed collection window time is used for each CBR flow. In the case of longer time to open collection window, the number of CTS packet being collected in DWSIGF is high compared to SIGF. The effect of given extra time on collection window in collecting the CTS packet increased the end to end delay of SIGF-priority, SIGF-random and DWSIGF-priority with 22, 19 and 20%, respectively as compared to IGF as shown in Fig. 9. It becomes more worst in DWSIGF-random where the delay almost double due to retransmission of packets when there is not enough CTS received because of less time allocated to open the collection window. On the other hand, even the performance on DWSIGF and SIGF slightly degrades when no attacker in the communication, this trade-off enhances the security aspect of the protocol itself while the attacker in the network.

In summary, the DWSIGF routing protocol adds extra overhead as compared to SIGF and IGF since, the dynamic collection time is used. The analysis is a baseline to investigate all the protocols under blackhole attack as the IGF is considered a perfect solution to be used when there is no attacker in the communication.

With blackhole attack: In this simulation, the blackhole attack is performed by the attacker A1 in Fig. 3 after CTS rushing attack is done. Once being selected as the forwarding node, the attacker sends a virtual ACK to sender to indicate the DATA is received correctly and will be transmitted to the required destination. However, all the packets received are actually dropped and not be relayed to the destination. As a result, the PDR will be zero percent. The experiment 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 sec^{-1}, thus for simplicity, existence of attacker is checked in this traffic rates only.

The chances of selecting the attacker as the forwarding node is reduced about 80 and 86% with DWSIGF-priority and DWSIGF-random, respectively as compared to IGF and SIGF-priority as shown in Fig. 10. This is because the approached used in DWSIGF (i.e., dynamic time allocated for collection window) make the collection window time is uncertainty to the attacker unless the attacker tries to be the first node reply with the CTS. In some of the cases, even the attacker try to be the first node who reply with the CTS, it's still no chance for them to give the CTS reply because of the small and unknown time allocated to open the collection window. With random selection of forwarding node in DWSIGF, it again reduced the selection of the attacker since, with less chance the attacker replied with the CTS and then it becomes a less chance for it to be selected even when it is being collected as the forwarding candidates. With the less possibility to choose the attacker thus, the PDR becomes better.

The DWSIGF-priority, SIGF-random and DWSIGF- random achieved mean of 65- 80% PDR even there is an attacker in the communication link with the DWSIGF-random performs 2 and 12% better as compared to SIGF-random and DWSIGF-priority, respectively as shown in Fig. 11, under traffic loads of 7 packets/sec/CBR flow. This will be a baseline result for

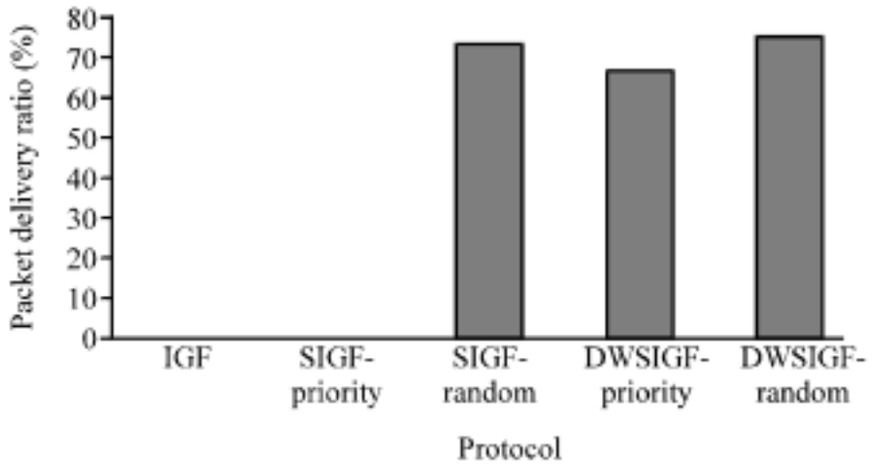

Fig. 11: Packet delivery ratio: blackhole attack

the next investigation when involved more than one attacker in the communication. However, IGF and SIGF-priority have a very bad performance on PDR with 0% PDR since, the attacker simply drops the entire received packet.

On the other hand, the DWSIGF still can provide a good PDR with mean of 80% even with the blackhole attack inline. This is due to less possibility to selects the attacker as the forwarding node as compared to SIGF and IGF.

CONCLUSIONS

In this study, the DWSIGF, the dynamic and secured routing protocol that resilience to blackhole and selective forwarding attack is presented. The simulation investigated the different time used to open the collection window for SIGF to find the suitable time for SIGF. It is then continued with the all protocols with priority and random selection with and without the attack as.

The DWSIGF either with priority or random selection is promising a minimal risk in selecting the attacker as the forwarding node. This will increase the network performance as a whole. As discussed before, blackhole and selective forwarding attacks can be grouped together because once attacker be selected as the forwarding node, it can do anything to the received packets, either drop all the received packets or selectively forward and drop certain packets.

This routing protocol also robust against wormholes, HELLO flood, sinkholes attacks and spoofing and altering of routing table even without any security techniques and mechanisms applied on it because it inherits the behavior of IGF routing strategies. 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 technique also limits the impact of attacks to local neighborhood only because the participating node is fully independent and dynamically chosen as late as possible. At the same time, with geographic routing properties, it is also resistant to insiders and outsiders' attackers since, it do not trust its neighboring nodes.

However, DWSIGF protocol still vulnerable to 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, the 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 study.

As a conclusion, the DWSIGF promise a good defense against blackhole and selective forwarding attack with better performance on PDR even without inserting any security mechanism inside the routing protocol. However, IGF still be a good solution when there is no attack in the network.

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

Abu, G.N., K. Kangand and K. Liu, 2005. Towards resilient geographic routing in WSNs. Proceedings of the 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Network, Oct. 13, ACM Press, USA., pp: 71-78.

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

Blum, B., T. He, S. Son and J. Stankovic, 2003. IGF: A state-free robust communication protocol for wireless sensor network. Technical Report CS-2003-11, University of Virginia. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.12.2828.

Hanapi, Z.M., M. Ismail, K. Jumari and H. Mirvaziri, 2008. Analysis of routing attacks in wireless sensor network. Proceedings of International Cryptology Workshop and Conference, Jun 9-12, Kuala Lumpur, pp: 202-214.

Hanapi, Z.M., M. Ismail, K. Jumari and M. Mahdavi, 2009. Dynamic window secured implicit geographic forwarding routing for wireless sensor network. Proc. World Acad. Sci., Eng. Technol. Int. Conf. Wireless Commun. Sensor Network, 39: 8-14.

He, T., B.M. Blum, K. Cao, J.A. Stankovic, H.S. Sang and T.F. Abdelzaher, 2007. Robust and timely communication over highly dynamic sensor networks. Real-Time Syst., 37: 261-289.

Huei, J.J. and I. Rubin, 2003. The Effect of Disengaging RTS/CTS dialogue in IEEE 802.11 MAC protocol. Proceedings of the International Conference on Wireless Networks, June 23-26, CSREA Press, Las Vegas, Nevada, USA., pp: 632-638.

Karlof, C. and D. Wagner, 2003. Secure routing in wireless sensor networks: Attacks and countermeasures. J. Ad Hoc Networks, 1: 293-315.

Kuo, C., M. Luk, R. Negi and A. Perrig, 2007. Message-in-a-bottle: User friendly and secure key deployment for sensor nodes. Proceedings of 5th International Conference on Embedded Networked Sensor Systems, Nov. 6-9, Sydney, Australia, pp: 233-246.

Newsome, J., E. Shi, D. Song and A. Perrig, 2004. The sybil attacks in sensor networks: Analysis and defense. Proceedings of 3rd International Symposium on Information Processing in Sensor Networks, (ISIPSN'2004), USA., pp: 259-268.

Qian, Y., K. Lu and D. Tipper, 2007. A design for secure and survivable wireless sensor networks. IEEE Wireless Commun., 15: 30-37.

Shi, J.F., X.X. Zhong and S. Chen, 2006. Study on communication mode of wireless sensor network based on effective result. J. Phys., 48: 1317-1321.

Wood, A.D. and J.A. Stankovic, 2002. Denial of service in sensor networks. IEEE Comput. Mag., 35: 54-62.

Wood, A.D., F. Lei, J., Stankovic and H. Tian, 2006. SIGF: A family of configurable, secure routing protocols for wireless sensor networks. Proceedings of the 4th ACM Workshop on Security Ad-hoc and Sensor Network, Oct. 30, ACM Press, Alexandria, Virginia, USA., pp: 35-48.

Yick, J.M. and D. Ghosal, 2008. Wireless sensor network survey. J. Comput. Network, 52: 2292-2330.