American J. of Engineering and Applied Sciences 2 (2): 494-500, 2009
ISSN 1941-7020

Priority and Random Selection for Dynamic Window Secured Implicit Geographic Routing in Wireless Sensor Network

Zurina Mohd Hanapi, Mahmod Ismail and Kasmiran Jumari
Department of Electrical, Electronics and Systems Engineering,
Faculty of Engineering and Built Environment,
University Kebangsaan Malaysia, Selangor, Malaysia

Abstract: Problem statement: Sensor nodes are easily exposed to many attacks since it were deployed in unattended adversarial environment with no global addressing and used for critical applications such as battlefield surveillance and emergency response. While the sensor also needs to act as a router to relay a message to a required recipient, then this increased the vulnerabilities to a network layer. However, existing security mechanisms are not permissible to be fitted directly into any sensor network due to constraints on energy and computational capabilities of sensor node itself that require on the modification on the protocols that associated with the sensor node itself in order to provide the security. **Approach:** In this study, a Dynamic Window Secured Implicit Geographic Forwarding (DWIGF) routing protocol was presented which based on an approach of lazy binding technique and dynamic time on collection window and inherits a geographical routing techniques. **Results:** The DWIGF was intelligent to minimize a Clear To Send (CTS) rushing attack and robust against black hole and selective forwarding attacks with high packet delivery ratios because of selection of a failed node and an attacker was minimized respectively. Moreover, few routing attacks were eliminated since the routing technique used was classified as geographic routing. **Conclusion:** This novel routing protocol was promising a secured routing without inserting any existing security mechanism inside.

Key words: Sensor network, routing security, dynamic window, routing attacks

INTRODUCTION

Secured routing ensures the message reaches a correct recipient in an accurate form and within a reasonable time delay. In Wireless Sensor Network (WSN), the sensor nodes have to do real time processing while responsible as a router to relaying message to the destination. However, in traditional network, the nodes that do the processing data are different from the communication nodes. Thus routing design for WSN becomes more challenging especially dealing with limited capabilities of sensor nodes (i.e., easily be destroyed, exhausted of energy or power, lower bandwidth, little processing power and limited sensing region[1,2]) that can caused a node failure. In WSN, node failure will result in inability to do its normal processing and fail to route the processing data to the destination. The capability constraints of sensor nodes also will cause any existing security mechanism developed for other networks cannot directly be applied into WSNs.

Node failure also can takes placed when there is an attacker during the communication. 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[1,3]. Attackers then can eavesdrop[1,4], inject bits and replay the packets at this layer especially in a wireless communication[2]. Thus, reduce the confidentiality and integrity[5] of the data being transmitted. Attackers can use many colluding nodes or can use more powerful device (i.e., laptop class attacker) 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.

Background: Routing Protocols: Routing technique is strongly dependent on the particular application (i.e., military, health, environmental and home) for which the

Corresponding Author: Zurina Mohd 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

WSN is used. In WSN, due to resource constraints of sensor nodes, IP-based routing protocol cannot be used. At the same time, design of routing protocol must be scalable to deal with different number of large deployed nodes in order to promise a network lifetime[2].

Generally, routing protocol in WSN can be classified into three different categories; flat, hierarchical and location based routing[6]. All nodes are typically assigned a same functionality and roles in the flat-based routing are different from hierarchical-based routing, where the nodes have different roles to play (i.e., Low Energy Adaptive Clustering Hierarchy (LEACH) by Heinzelman *et al*.[7]). 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*.[8] and IGF[9]). The position of a node can be relative to its neighbors or absolute 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 Dynamic Window Secured Implicit Geographic Forwarding (DWSIGF) is categorized as location-based routing (i.e., geographic routing) since it inherits the behavior of Secured Implicit Geographic Forwarding (IGF) and Window Secured Implicit Geographic Forwarding (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

Routing security: In WSN, the network must be resilient to individual node failure[8] in order to maintain the network availability and successful transmission. Zero power energy[1] and attacks as discussed by Wood *et al*.[10] are the serious issues that caused the node died. In this study, only security issue is taken into consideration for the DWSIGF implementation since existing security mechanism cannot be directly fitted into WSN and improvement of routing strategies can be one of solution to provide the secured routing. However, energy consumption still minimal[11] in DWSIGF since it use multihop routing.

The DWSIGF inherits the behaviors of IGF, then few of routing attacks that has been studied by Karl of and Wagner[1], Wood *et al*.[10] and Gupta[3] (i.e., state corruption, wormholes attack, HELLO floods attack, black holes attack, selectively forwarding attack, Sybil attacks[12] and Denial of Service (DoS)) attacks[13] are indirectly eliminated.

The DWSIGF also keeps no routing table since the forwarding node is computed with lazy binding approach[9] where the hop node is calculated as late as possible when there is only a packet to send. Thus as discussed by Wood *et al*.[10], it is protected from the routing state corruption while minimize the use of energy and memory. At the same time, DWSIGF also free from the HELLO floods, wormholes and sinkholes attack as it is based on geographic routing[10]. 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 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[14], black hole attack, selective forwarding attack and DoS attack. A Sybil node could appear in more than one place at once[10] with different set of nodes or virtual locations. Location verifications can be done on each node as suggested by attacks[9,14] 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 Karlof and Wagner[1].

Selective forwarding and black holes attacks can be group together based on[1,3]. 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, the attacker is always being selected as the participating node because they perform 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.

Implicit geographic forwarding routing protocol: Stateless routing used by IGF and SIGF attracts the DWSIGF to inherit the approach since memory and expensive communication can be minimized without the need of routing table. At the same time, the lazy binding technique used also make the protocol 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, this

minimized the chance of a packet to be relayed to the nodes that are moved out of range, died, or in sleep state. Thus minimized the used of energy and promise fault tolerance[15], to resent a control packet to find the participating node.

According to Blum *et al.*[9], IGF routing protocol used hybrid network/Medium Access Control (MAC) protocol. 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 in wireless communication[15]. The communication hand-shake 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 carrier sense a channel for DCF Inter-Frame Spacing (DIFS) time. The sender S then broadcast an Open RTS (ORTS) containing location of S and D if the channel is free after the DIFS time.

The 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 packet as shown in Fig. 2. CTS packet contains a location of candidate nodes. They have to set a CTS Response time[9,15] (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 the CTS. On the expiry of the timer, they will reply with 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 who have the less CTS Response time will reply the CTS. Thus, as shown in Fig. 2 the R is be selected as the forwarding nodes in order to relay a DATA to the destination. The process continues with multi hop communication until the destination D sent an acknowledgement.

Secured implicit geographic forwarding routing protocol: SIGF also inherits some of the behaviors of IGF but the focus on the improvement of routing security. It founds that without routing table, it gives zero possibility to alter and spoof routing information. However, only with a single attacker in IGF, it can completely corrupt the routing for all of its neighbors. This is happen when the attacker is chosen as the forwarding node after the candidates nodes be the first node reply with the CTS immediately after received the ORTS in any of the hop count. 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 or selectively forward the DATA packet to the next hop or destination.

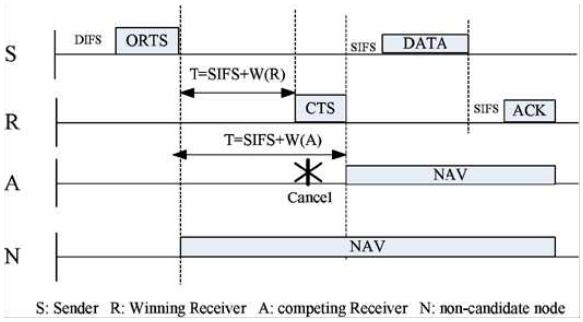

Fig. 1: IGF hand-shake timeline[15]

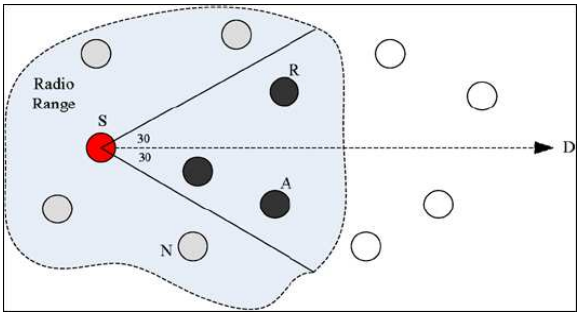

Fig. 2: Forwarding area, 60° sextants centered on the direct line with respect to the destination[15]

In that case, SIGF overcomes the chances of attacked by verify all the CTSs received. In this case, all candidates within 60° 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 priority selection, attackers again be selected as the forwarding nodes that lead to another routing attacks as well.

MATERIALS AND METHODS

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

The DWSIGF's aim is to minimize the change of attacker to take part on the communication. Unlike SIGF, random time is targeted to minimize the chances

of adversaries to take part as the hop node since they do not know an exact time the collection window is open. We will open to so many respondents of the CTS packet and verify its location and its remaining energy 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 it is selected by the sender, the communication continues with 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 with the method first come first be selected, fixed time and dynamic time respectively. The discussed communication process is elaborated in general pseudo code below without the detail of communication handshake timeline and MAC IEEE 802.11 semantic:

```
/*sender*/
if (sender have packet to send)
    broadcast ORTS (S_Location, D_Location);
    set ORTS wait timer;
    C_candidates ← Ø
    Set random time for collection window;
    /*re-open collection window if time allocated not
    enough to collect any C_candidates */
    while (collection window open)
       if ( CTS received AND S_Location ∈ forwarding
       area)
          Add N to C_candidates;
    Choose R ∈ C_candidates for next hop;
    ACK received;

/*neighbors and receiver */
if (neighbor received ORTS packet)
    if (neighbor within FWDArea)
       set CTS response timer;
          send CTS (N_Location) upon expiry of CTS
          response time;
    else
       set NAV based on 802.11;
```

Simulation: 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.

Table 1: System parameters for simulation

Terrain	150×50 m
Number of nodes	196
Node placement	Grid + Ɒ(0,16) noise
Application	CBR streams
Payload size	32 bytes
Simulation length	100 packets, 10 runs
Radio range	40 m
Radio bandwidth	200 kbps
W_P	2
W_R	1

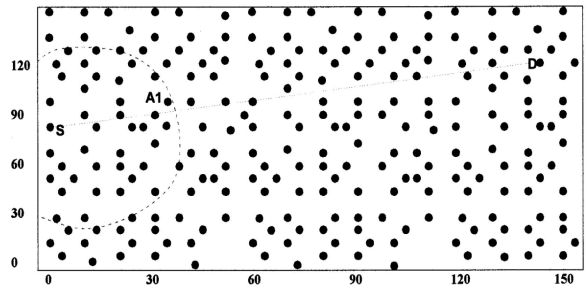

Fig. 3: Deployement of 196 nodes with sender S, destination D and attacker A1

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

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 shown 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 ten times. The result is a mean of ten simulation runs.

The simulation involved 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 six senders situated at the left side of the region and two receivers at the right of the region.

The experiments 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.

The simulation on attack only used one attacker to perform the black hole attacks that caused by the CTS rushing attack. Fig. 3 shows the sender, destination and attacker A1 used in the experiments.

RESULTS

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

Without attack: Figure 4-6 shows results without attack done on IGF, SIGF (with priority selection) and DWSIGF (with priority selection and random 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 attacker performs the attacks.

Figure 4 shows IGF, SIGF-priority, SIGF-random, DWSIGF-priority and DWSIGF-random have comparable delivery ratios (95-100) % under light traffic load. When the traffic starts to flow with rates 7 packets sec^{-1}, each protocol starts to suffer congestion. SIGF-priority, SIGF-random, DWSIGF-priority and DWSIGF-random degrade 0.02, 0.01, 4 and 3% respectively to IGF because of the protocols allow additional time to collect multiple CTS packet.

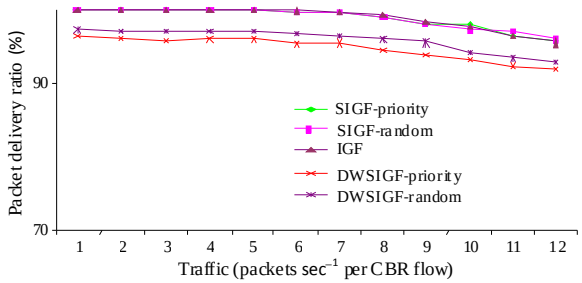

Fig. 4: Packet Delivery Ratio (PDR): Without attack

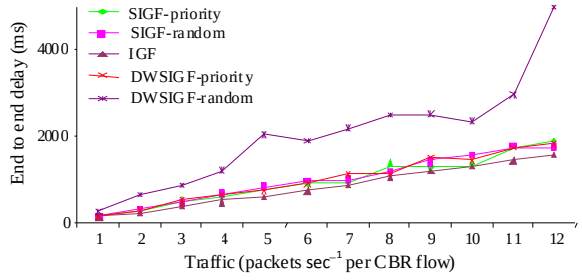

Fig. 5: End to end delay: Without attack

In SIGF, fixed collection window time is used for each CBR flows; however DWSIGF used dynamic window time. In the case of longer time to open collection window is used for any of the communication flows, thus 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 have minimal increment on the end to end delay of SIGF-priority, SIGF-random and DWSIGF-priority with 17, 20 and 20% respectively when compared to IGF as shown in Fig. 5. However the DWSIGF-random increased almost double on the end to end delay due to retransmission of packet when there is not enough CTS received because of less time allocated to open the collection window. Nevertheless, this trade-of enhances the security aspect of the protocol itself.

The SIGF and DWSIGF used all the control packets (i.e., used MAC control packets; ORTS, CTS and ACK) of IGF to carry out the communication. Therefore, there is no big different on the communication overhead even in heavy traffic load as shown in Fig. 6 except extra CTS packets are sent in SIGF-priority, SIGF-random and DWSIGF-priority depending on the time allocated for the collection window that results in 4, 5 and 5% increment respectively with respect to IGF. However, with random selection done on DWSIGF, the communication overhead almost double because of retransmission of control packets to reinitiate the communication when not enough CTS collected during the open time of collection window.

In summary, DWSIGF adds extra overhead compared to SIGF and IGF since dynamic collection time is used. This is just a baseline to investigate the protocols under black hole attack. However, the IGF considered a perfect solution to be used when there is no attacker in the communication.

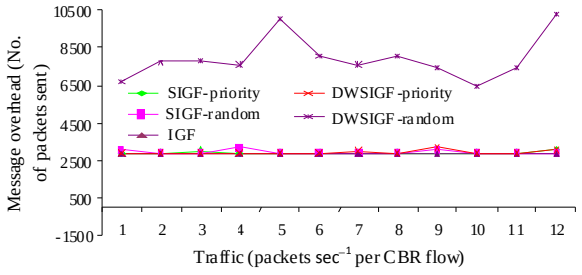

Fig. 6: Message overhead: Without attack

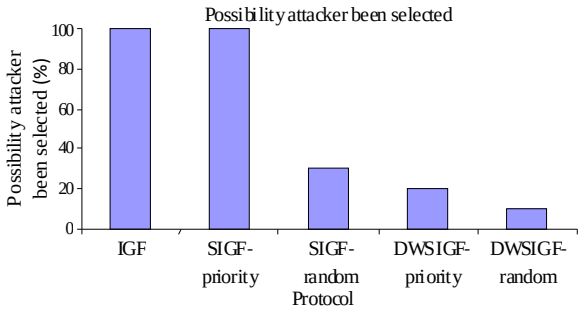

Fig. 7: Possibility of selecting attacker as forwarding node

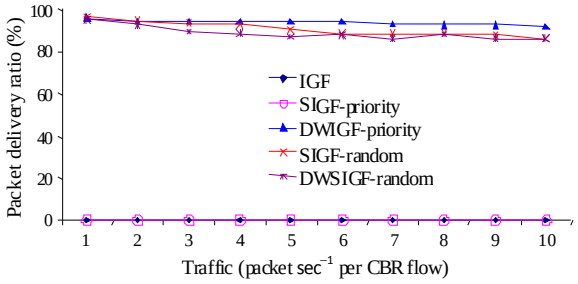

Fig. 8: Packet delivery ratio: Black hole attack

With black hole attack: In this simulation, black hole attack is created when the attacker A1 in Fig. 3 performs the CTS rushing attack. Once being selected as the forwarding node, then it sends a virtual ACK to indicate the DATA is already received and will be transmitted to the required destination but actually all the packets received are actually dropped and is 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.

Figure 7 shows with approached used in DWSIGF (i.e., dynamic time allocated for collection window), the chances of selecting the attacker as the forwarding is reduced about 80 and 90% with DWSIGF-priority and DWSIGF-random respectively as compared to IGF and SIGF-priority. This is because the closed time of the collection window 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 in DWSIGF, it again reduced the selection of the attacker since with less chance the attacker replied with 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.

Figure 8 shows PDR for IGF, SIGF and DWSIGF under increasing traffic loads. The DWSIGF-priority, SIGF-random and DWSIGF-random achieved mean of 90-95% PDR even there is an attacker in the communication link with the DWSIGF-priority performs better 4-5% compared to SIGF-random and DWSIGF-random. This will be a bench mark for the next investigation when involved more than one attackers in the network. However, IGF and SIGF-priority have a very bad performance on PDR since the attacker simply drop the entire received packet.

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

DISCUSSION

The dynamic time used in DWSIGF (either with priority or random selection) promising a minimal risk in selecting attacker as the forwarding node caused by the CTS rushing attack and the chances of having the black hole and selective forwarding attack is reduced particularly. Once the attacker is not able to take part in the communication, thus the communication process is continued with the right protocol semantics which leads to better network performance.

The DWSIGF-random can be use to minimize the possibility to select the attacker as the hop node, however to have the better PDR, the DWSIGF-priority is the best choice to use. Nevertheless, DWSIGF 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.

CONCLUSION

In this study, the DWSIGF, the dynamic window stateless routing protocol that resilience to black hole and selective forwarding attack caused by the CTS rushing attack is presented. Even without inserting any security mechanism inside the routing protocol, the DWSIGF still promise a good defense against black hole attack with good network performance. The DWSIGF inherits resistance to 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 since it inherit the behavior of IGF and SIGF strategies. Moreover, it limits the impact of attacks to just a local neighborhood 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, IGF still be a good solution when there is no attack in the network. Future research could evaluate 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 research was supported by research grant UKM-OUP-NBT-29-153/2008.

REFERENCES

1. Karlof, C. and D. Wagner, 2003. Secure routing in wireless sensor networks: Attacks and countermeasures. J. Ad Hoc Networks, 1: 293-315. http://dx.doi.org/10.1016/S1570-8705(03)00008-8
2. Yick, J.M. and D. Ghosal, 2008. Wireless sensor network survey. J. Comput. Network, 52: 2292-2330. DOI: 10.1016/j.comnet.2008.04.002
3. Gupta, S., 2006. Automatic Detection of DOS Routing Attacks in Wireless Sensor Networks, MSc Thesis, Wireless System Research Group (WiSeR) Publication. http://wireless.cs.uh.edu/publications/files/sumit_thesis-fa06
4. 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, pp: 233-246. http://doi.acm.org/10.1145/1322263.1322286
5. Qian, Y., K. Lu and D. Tipper, 2007. A design for secure and survivable wireless sensor networks. IEEE wireless commun., 15: 30-37. http://dx.doi.org/10.1109/MWC.2007.4396940
6. Al Karaki, J.N. and A.E. Kamal, 2004. Routing techniques in wireless sensor networks: A survey. IEEE Wireless Commun., 11: 6-28. DOI: 10.1109/MWC.2004.1368893
7. Heinzelman, W.R., A. Chandrakasan and Balakrishnan, 2000. Energy-efficient communication protocol for wireless sensor networks. Proceedings of 33rd Annual Hawaii International Conference on System Sciences, Jan. 4-7, IEEE Xplore Press, USA., pp: 1-10. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?isNumber=20043&arNumber=926982&isnumber=20043&arnumber=926982
8. Wood, A.D. and J.A. Stankovic, 2002. Denial of service in sensor networks. IEEE Comput. Mag., 35: 54-62. http://dx.doi.org/10.1109/MC.2002.1039518
9. 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
10. 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. 30-30, ACM Press, Alexandria, Virginia, USA., pp: 35-48. http://doi.acm.org/10.1145/1180345.1180351
11. 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. DOI: 10.1088/1742-6596/48/1/245
12. 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, pp: 259-268. DOI: 10.1109/IPSN.2004.1307346
13. Wood, A.D. and J.A. Stankovic, 2002. Denial of service in sensor networks. IEEE Comput. Mag., 35: 54-62. DOI: 10.1109/MC.2002.1039518
14. 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. 13-13, ACM Press, USA., pp: 71-78. http://doi.acm.org/10.1145/1089761.1089774
15. 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. J. Real-Time Syst., 37: 261. DOI: 10.1007/s11241-007-9025-2