International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 3

Data Prevention from Network Hacking

A Prasanth, P Sankar Ganesh, S P Raja Gopalan
Department of Computer Science and Engineering, G.K.M. College
of Engineering and Technology, Chennai, Tamil Nadu, India

ABSTRACT

We are sending data from source node to destination using wireless sensor networks (WSNs), In wireless sensor networks, it is a typical threat to source privacy that an attacker performs back tracing strategy to locate source nodes by analyzing transmission paths. So there is lot of chances to lose data and information theft by network hackers. Network hackers performs eves dropping, sniffers attack, Denial of service attack. These types of attacks are achieved by negative commands generated by intermediate server maintained by hackers. With the popularity of the Internet of Things (IoTs) in recent years, source privacy protection has attracted a lot of attentions. However, they fail to get the tradeoff between multi-path transmission and transmission cost. In this project, we propose a Constrained Random Routing (CRR) mechanism and Greedy techniques, which can constantly change routing next-hop instead of a relative fixed route so that attackers cannot analyze routing and trace back to source nodes. At first we designed the randomized architecture for each sensor nodes. Then calculate the coordinates and weights of node, Finally, the selected weights help to decide which node will become the next hop. In this way, attackers would be confused by the constantly changing paths. The simulation results prove that our proposal can achieve high routing efficiency in multi-path transmission.

Keywords: *wireless network sensor (WNS), Internet of Things (IOT) , Constrained Random Routing (CRR) mechanism, Greedy techniques, Network Utility Maximinization (NUM), Distributed algorithm, Traffic allocation algorithm*

INTRODUCTION

The project propose techniques for the network nodes to estimate and characterize the impact of Hacking and source node failure. we consider the problem of Problem free data transfer in network node routing in which the source node performs traffic allocation based on empirical jamming statistics and dynamic routing at individual network nodes to prevent data loss. Different from traditional wired network WNS as usually deployed in unnamed area .if it is have density complex data encryption algorithm has already has been used . The attacker usually uses expensive wireless receives to determine the position of signals transmitting node and the move to the node to monitor continuously, repeating the procedure the attacker can perform back tracking strategy to find the position of the source node, we found on improving the efficiency of source privacy protection . from this paper constrained random routing (CRR) based on the transmitting offset angles and constrained probability is proposed to protect the privacy of source node CRR fully consider energy consumption in multipath transmission and also using methodology of Network utility maximization , Greedy random walk (GROW) mainly used for proposed traffic allocation method also distributed algorithm are mainly required application area of distributed system and it also distributed information process . In this paper they are proposed to incorporate the jamming impact in the allocation problem the effect of jamming on transmission are each link , they are stop the backtracking and change their sequence the import of jamming dynamic and mobility on network throughput , the multiple path source routing

RELATED WORKS

1. H. GuangJie, J. Jinfang, M. Guizani, and J. J. Rodrigues in 2016, Green routing protocols for wireless multimedia sensor networks, for Real-time critical multimedia requires efficient routing for data delivery with guaranteed QoS .
2. W. Cho and M. Shaw in 2013, HySense: A hybrid mobile crowd sensing framework for sensing opportunities compensation under dynamic coverage constraint. Crowd sensing applications are driven by sufficient users, advanced incentive mechanisms have been designed to enhance users' willingness to participate in sensing tasks.
3. W. Cho and M. Shaw in 2017 , A disaster management-oriented path planning for mobile anchor node-based localization in wireless sensor networks , for The localization of sensor nodes is a significant issue in wireless sensor networks (WSNs) because many applications cannot provide services without geo location data, especially during disaster management.
4. K. Pandurang, Z. Yanyong, T. Wade, and O. Celal in 2005, Enhancing source-location privacy in sensor network routing , Although many privacy-related issues can be addressed by security mechanisms, one sensor network privacy issue that cannot be adequately addressed by network security is source-location privacy.
5. P. Kanthakumar and L. Xiao in 2011, maintaining source privacy under eaves-dropping and node compromise attacks.
6. Y. Xi, L. Schwiebert, and W. Shi in 2016, Preserving source location privacy in monitoring-based wireless sensor networks.
7. J. Ren and D. Tang in 2011, Combining source-location privacy and routing efficiency in wireless sensor networks.

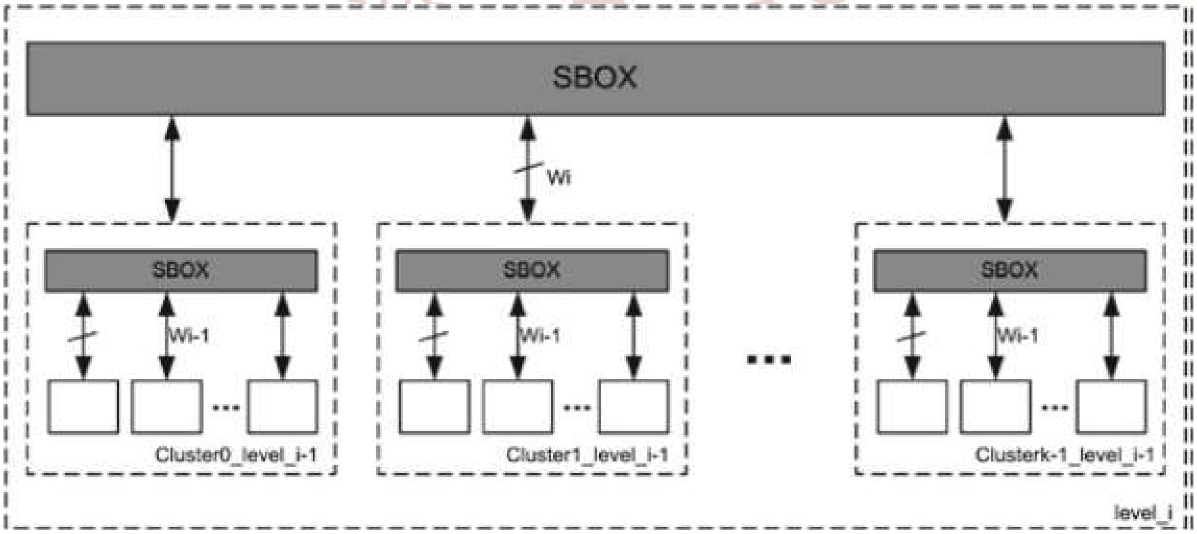
PROPOSED SYSTEM

In order for a source node s to incorporate the jamming impact in the traffic allocation problem, the effect of jamming on transmissions over each link (i,e) It must be estimated and relayed to s. However, to capture the jammer mobility and the dynamic effects of the jamming attack, the local estimates need to be continually updated. We begin with an example to illustrate the possible effects of jammer mobility on the traffic allocation problem and motivate the use of continually updated local estimates.

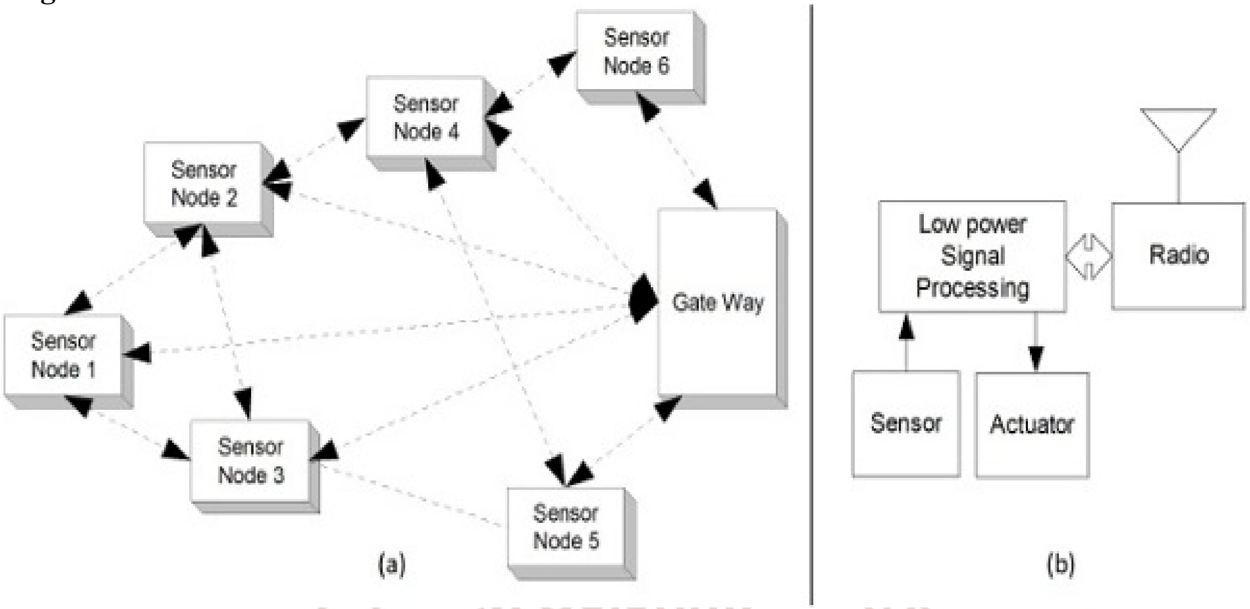
Advantage:

1. WSNS support ad hoc networking, and have the capability of self-forming, self-healing, and self-organization.
2. Mesh routers have minimal mobility and perform dedicated routing and configuration, which significantly decreases the load of mesh clients and other end nodes.
3. Mobility of end nodes is supported easily through the wireless infrastructure. Mesh routers integrate heterogeneous networks, including both wired and wireless. Thus, multiple types of network access exist in WSNS

Architecture Diagram



Block Diagram:



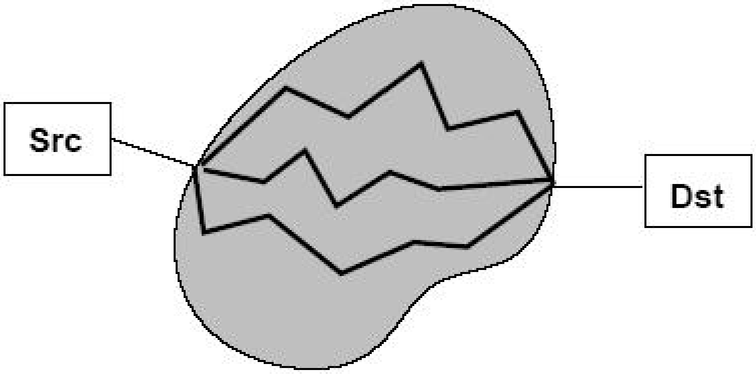
(a) Typical wireless sensor network scenario

(b) Sensor node block diagram

MULTIPLE PATH ROUTING ALGORITHM

Multipath Routing is the spreading of traffic from a source node to a destination node over multiple paths through the network. This algorithm is to design an optimising intra-domain routing protocol which is not constrained by weight-tuning, and which can be implemented with minor modifications of the legacy forwarding mechanism based on destination address prefix. This project present a routing algorithm for such a protocol based on multi-commodity flow optimization which is both computationally tractable for on-line optimization and also can be implemented with a near-legacy forwarding mechanism.

MULTIPATH ROUTING DESIGN:



SOURCE ROUTING ALGORITHM

Source routing, also called path addressing, allows a sender of a packet to partially or completely specify the route the packet takes through the network.[1] In contrast, in non-source routing protocols, routers in the network determine the path based on the packet's destination. Source routing allows easier troubleshooting, improved traceroute, and enables a node to discover all the possible routes to a host. It does not allow a source to directly manage network performance by forcing packets to travel over one path to prevent congestion on another.

POINT THE EFFECT OF JAMMER MOBILITYON NETWORK

Providing a set of parameters to be estimated by network nodes and methods for the sources to aggregate this information and characterize the available paths on the basis of expected throughput.

ESTIMATING LOCAL PACKET SUCCESS RATES

The up- date period T and update relay period Ts between subsequent updates of the parameter estimates have significant influence on the quality of the estimate. If the update period Ts is too large, the relayed estimates will be outdated.

ESTIMATING END-TO-END PACKET SUCCESS RATES

The source needs to estimate the effective end-to-end packet success rate to determine the optimal traffic allocation. Assuming the total time required to transport packets from each source to the corresponding destination is negligible compared to the update relay period.

TRAFFIC ALLOCATION CONSTRAINTS

We must consider the source data rate constraints, the link capacity constraints, and the reduction of traffic flow due to jamming at intermediate nodes

OPTIMAL TRAFFIC ALLOCATION USING PORTFOLIO SELECTION THEORY

To determine the optimal allocation of traffic to the paths in Portfolio Selection, each source s chooses a utility function that evaluates the total data rate, or throughput, successfully delivered to the destination node

CONCLUSIONS

We studied the problem of traffic allocation in multiple-path routing algorithms in the presence of jammers whose effect can only be characterized statistically. We have presented methods for each network node to probabilistically characterize the local impact of a dynamic jamming attack and for data sources to incorporate this information into the routing algorithm. We formulated multiple-path traffic allocation in multi-source networks as a lossy network flow optimization problem using an objective function based on portfolio selection theory from finance. We showed that this centralized optimization problem can be solved using a distributed algorithm based on decomposition in network utility maximization (NUM). We presented simulation results to illustrate the impact of jamming dynamics and mobility on network throughput and to demonstrate the efficacy of our traffic allocation algorithm. We have thus shown that multiple path source routing algorithms can optimize the throughput performance by effectively incorporating the empirical jamming impact into the allocation of traffic to the set of paths.

REFERENCES

1. P. Hui, C. Hong, Z. XiaoYing, F. YongJian, L. CuiPing, and L. DeYing, ‘‘Location privacy preservation in wireless sensor networks,’’ *J. Softw.*, vol. 26, no. 3, pp. 617–639, 2015.
2. H. GuangJie, J. Jinfang, M. Guizani, and J. J. Rodrigues, ‘‘Green routing protocols for wireless multimedia sensor networks,’’ *IEEE Wireless Commun. Mag.*, vol. 23, no. 6, pp. 140–146, Dec. 2016.
3. G. Han, L. Liu, S. Chan, R. Yu, and Y. Yang, ‘‘HySense: A hybrid mobile crowd sensing frame work for sensing opportunities compensation under dynamic coverage constraint,’’ *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 93–99, Mar. 2017.
4. H. GuangJie, Y. Xuan, L. Li, Z. WenBo, and M. Guizani, ‘‘A disaster management-oriented path planning for mobile anchor node-based localization in wireless sensor networks,’’ *IEEE Trans. Emerg. Topics Comput.*, to be published.
5. K. Shin, K. Kim, and S. Kim, ‘‘ADSR: Angle-based multi-hop routing strategy for mobile wireless sensor networks,’’ in *Proc. IEEE Asia–Pacific Services Computer. Conf.*, Dec. 2011, pp. 373–376.
6. P. Spachos, D. Toumpakaris, and D. Hatzinakos, ‘‘Angle-based dynamic routing scheme for source location privacy in wireless sensor networks,’’ in *Proc. Veh. Technol. Conf.*, May 2015, pp. 1–5.
7. Z. ZeMao, L. Yang, Z. Fan, Z. JianQin, and Z. Pin, ‘‘Research on source location privacy routing based on angle and probability in wireless sensor

networks,'' *J. Shandong Univ.*, vol. 48, no. 9, pp. 1–9, 2013.

8. W. Choi, S. K. Das, and K. Basu, ''Angle-based dynamic path construction for route load balancing in wireless sensor networks,'' in *Proc. IEEE Wireless Commun. Netw. Conf.*, vol. 4. Mar. 2004, pp. 2474–2479.
9. Z. YaNan, Y. Xong, and X. Wu, ''Enhanced source-location privacy preservation protocol using random angle,'' *Computer Engineering and Applications*. 2016.