IJRRECS/December 2013/Volume-1/Issue-8/1893-1898 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

AN APPROACH TOWARDS SECLUDED DATA COLLECTION IN WIRELESS NETWORKS

Yandrapati Ashok Kumar[1], L.Veera Babu[2]

[1]M.Tech Student, Dept of CSE, TRR College of Engineering, Patancheru, Medak Dist, A.P, India

[2]Assistant Professor, Dept of CSE, TRR College of Engineering,Patancheru, Medak Dist, A.P, India

ABSTRACT:

Among the variety of possible security threats which are encountered in a wireless sensor network, two types of attacks are particularly interested in combating such as compromised node as well as denial of service. Due to the unattended environment of wireless sensor network adversaries can effortlessly construct black holes. When taking into consideration the stringent constraint on energy expenditure in wireless sensor networks, the major challenge in our design is to create extremely dispersive random routes at low energy expenditure. A randomized multipath routing algorithm was introduced in which numerous paths are computed in a method of randomized every time an information packet desires to be sent, so that the set of routes engaged by a variety of shares of various packets remain altering over time. The algorithm can be functional to selective packets in wireless sensor networks to make available levels of additional security in opposition to adversaries attempting to get hold of these packets.

Keywords: Wireless sensor network, Adversary, Randomized multipath routing algorithm.

1. INTRODUCTION:

The notion of multipath routing dates back, when it was primarily introduced to extend the traffic intended for the purpose of load balancing in addition to throughput enhancement and afterwards, path-disjoint multipath routing, has paying attention a lot of concentration in wireless networks appropriate to its robustness in combating issues of security [4]. The variety of possible

security threats which are encountered in a wireless sensor network, two types of attacks are particularly interested in combating such as compromised node as well as denial of service. In the attack of compromised node, an adversary actually compromises a subset of nodes towards the data of eavesdrop, whereas in attack of denial of service, the adversary impedes with the regular operation of the network by means of dynamically disrupting, altering, or still paralyzing the functionality of a nodes subset [8]. These two attacks are comparable in the intellect that they both produce black holes: regions within which the adversary moreover inactively intercept or else actively obstruct the information delivery. Due to the unattended environment of wireless sensor network adversaries can effortlessly construct black holes. Severe compromised node as well as denial of service attacks can interrupt normal delivery of data connecting sensor nodes and the sink, otherwise even division the topology [1]. A conventional method of cryptography-based security cannot alone make available acceptable solutions to these troubles. Once a node is settled, the adversary can forever obtain the keys of encryption/decryption keys of that node, and consequently can interrupt any information accepted through it [12]. An adversary can forever carry out attacks of denial of service even if it does not contain any information of the fundamental cryptosystem. A randomized multipath routing algorithm was introduced in which numerous paths are computed in a method of randomized every time an information packet desires to be sent, so that the set of routes engaged by a variety of shares of various packets remain altering over time [3]. As a result, a great number of routes can be potentially produced for each source in addition to destination. To intercept various packets, the adversary has to cooperate otherwise jam all probable routes from the source towards the destination, which is almost not achievable. For the reason that routes are at present arbitrarily generated, they may possibly no longer be present node-disjoint [14]. The algorithm makes sure that the routes which are arbitrarily generated are as dispersive as probable; specifically the routes are geographically detached as far as promising such that they include high probability of not concurrently passing all the way through a black hole [9]. When taking into consideration the stringent constraint on energy expenditure in wireless sensor

networks, the major challenge in our design is to create extremely dispersive random routes at low energy expenditure. The proposed algorithm can be functional to selective packets in wireless sensor networks to make available levels of additional security in opposition to adversaries attempting to get hold of these packets [7]. By regulating the random propagation in addition to the parameters of secret sharing levels of different security can be made available by the algorithm at altered energy expenditure. When taking into consideration that the percentage of packets in a wireless sensor network that need a level of high security is minute, it was believed that the selective usage of the proposed algorithm does not considerably impact the energy competence of the complete system [2].

2. METHODOLOGY:

An approach of three-phase is intended for secure information delivery within a wireless sensor secret sharing of data, randomized propagation of each share of information, in addition to normal routing toward the sink [12]. A randomized multipath routing algorithm was introduced in which numerous paths are computed in a method of randomized every time an information packet desires to be sent, so that the set of routes engaged by a variety of shares of various packets remain altering over time. When a node of sensor desires to send a packet towards the sink, it initially breaks the packet into M shares, in accordance with (T, M) an algorithm of threshold secret sharing algorithm [5]. Every share is subsequently transmitted towards several randomly selected neighbor and that neighbor will carry on to transmit the share it has received to former randomly selected neighbors. In every share, there is a field of TTL, whose early value is set by means of the source node to manage the total number of haphazard relays. Subsequent to each relay, the fields of TTL is condensed by 1. When the value of TTL reaches 0, the last node to accept this share commences to route it toward the sink by means of min-hop routing [10]. Once the sink collects not less than shares of T, it can rebuild the original packet. No data can be improved from not more than shares of T. The consequence of route dispersiveness on circumventing black holes is shown in fig1, where the dotted circles correspond to the ranges the secret shares can be transmitted to in the phase of random propagation. A

larger dotted circle entails that the resultant routes are geographically more dispersive [6]. The routes of advanced dispersiveness are more competent of evading the black hole. The phase of random propagation is the important component that dictates the protection and energy performance of the entire method. To expand routes, an ultimate algorithm of random propagation would transmit shares as dispersively as probable [13]. When taking into consideration that the percentage of packets in a wireless sensor network that need a level of high security is minute, it was believed that the selective usage of the proposed algorithm does not considerably impact the energy competence of the complete system. At the same time, it is extremely attractive to have an energy-efficient transmission, which calls for restraining the number of haphazardly propagated hops. The challenge here lies in the unsystematic and dispersed nature of the propagation: a share may possibly be sent one hop beyond from its source in a specified step, but may possibly be sent reverse closer towards the source in the subsequent step, wasting both steps from a safety point of view. To undertake this issue, several control requirements to be forced on the process of random propagation.

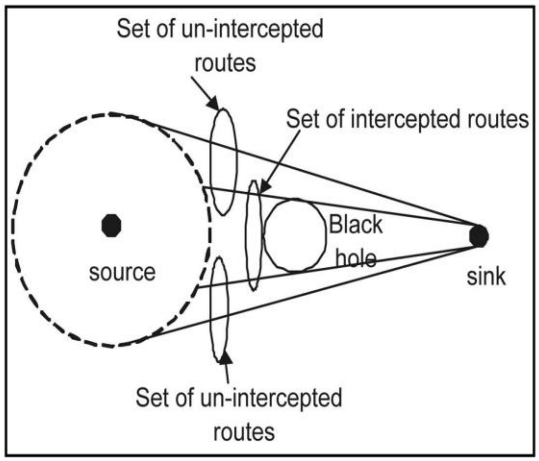

Fig1: An overview of inference of route dispersiveness.

3. RESULTS:

To better appreciate the capability of the algorithms of randomized multipath routing in bypassing black holes, their performance against a deterministic counterpart, H-SPREAD which produces node-disjoint multipath routes towards combating attacks of compromised node in wireless sensor networks were compared. The nodes' locations contain an important impact on the complete value of the packet interception likelihood of a given method. It was emphasized that when reading the, the complete value of the mean performance is not as helpful as the comparative performance ranking among a variety of schemes, and also not as helpful as the

common trend in performance. Provided that the nodes are consistently distributed, the modification of node density does not impact the size of these circles otherwise the allotment of the shares more than these circles. The packet interception likelihood of H-SPREAD decreases considerably with the boost in density of node, for the reason that additional node-disjoint routes can be initiated.

4. CONCLUSION:

Path-disjoint multipath routing, has paying attention a lot of concentration in wireless networks appropriate to its robustness in combating issues of security. An approach of three-phase is intended for secure information delivery within a wireless sensor secret sharing of data, randomized propagation of each share of information, in addition to normal routing toward the sink. It was emphasized that when reading the, the complete value of the mean performance is not as helpful as the comparative performance ranking among a variety of schemes, and also not as helpful as the common trend in performance. By regulating the random propagation in addition to the parameters of secret sharing levels of different security can be made available by the algorithm at altered energy expenditure.

REFERENCES:

[1] T. Claveirole, M.D. de Amorim, M. Abdalla, and Y. Viniotis, "Securing Wireless Sensor Networks Against Aggregator Compromises,"
IEEE Comm. Magazine, vol. 46, no. 4, pp. 134-141, Apr. 2008.

[2] W. Lou, W. Liu, and Y. Zhang, "Performance Optimization Using Multipath Routing in Mobile Ad Hoc and Wireless Sensor Networks," Proc. Combinatorial Optimization in Comm. Networks,
pp. 117-146, 2006.

[3] B. Vaidya, J.Y. Pyun, J.A. Park, and S.J. Han, "Secure Multipath Routing Scheme for Mobile Ad Hoc Network," Proc. IEEE Int'l Symp. Dependable, Autonomic and Secure Computing, pp. 163-171, 2007.

[4] P.C. Lee, V. Misra, and D. Rubenstein, "Distributed Algorithms for Secure Multipath Routing in Attack-Resistant Networks," IEEE/
ACM Trans. Networking, vol. 15, no. 6, pp. 1490-1501, Dec. 2007.

[5] M.K. Marina and S.R. Das, "On-Demand Multipath Distance Vector Routing in Ad Hoc Networks," Proc. IEEE Int'l Conf. Network Protocols (ICNP), pp. 14-23, Nov. 2001.

[6] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks,"

IEEE Comm. Magazine, vol. 40, no. 8, pp. 102-114, Aug. 2002.

[7] W. Lou and Y. Kwon, "H-Spread: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks," IEEE Trans. Vehicular Technology, vol. 55, no. 4, pp. 1320- 1330, July 2006.

[8] D.B. Johnson, D.A. Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks," Ad Hoc Networking, C.E. Perkins, ed., pp. 139-172, Addison-Wesley, 2001.

[9] C.L. Barrett, S.J. Eidenbenz, L. Kroc, M. Marathe, and J.P. Smith, "Parametric Probabilistic Sensor Network Routing," Proc. ACM Int'l Conf. Wireless Sensor Networks and Applications (WSNA), pp. 122-131, 2003.

[10] Z. Ye, V. Krishnamurthy, and S.K. Tripathi, "A Framework for Reliable Routing in Mobile Ad Hoc Networks," Proc. IEEE INFOCOM, vol. 1, pp. 270-280, Mar. 2003.

[11] M. Burmester and T.V. Le, "Secure Multipath Communication in Mobile Ad Hoc Networks," Proc. Int'l Conf. Information Technology:
Coding and Computing, pp. 405-409, 2004.

[12] P. Papadimitratos and Z.J. Haas, "Secure Routing for Mobile Ad Hoc Networks," Proc. SCS Comm. Networks and Distributed Systems Modeling and Simulation Conf. (CNDS), 2002.

[13] P.C. Lee, V. Misra, and D. Rubenstein, "Distributed Algorithms for Secure Multipath Routing," Proc. IEEE INFOCOM, pp. 1952-
1963, Mar. 2005.

[14] W. Lou, W. Liu, and Y. Fang, "Spread: Enhancing Data Confidentiality in Mobile Ad Hoc Networks," Proc. IEEE INFOCOM, vol. 4, pp. 2404-2413, Mar. 2004.