Tushar Agarwal, Dr. Raj Kumar, Hitesh Rajvanshi, Dr. Sohan Garg/ International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 1, Issue 3, pp.974-985

Design and Development of a Secured Routing Scheme for Wireless Sensor Networks

Tushar Agarwal[1], Dr. Raj Kumar[2], Hitesh Rajvanshi[3], Dr. Sohan Garg[4]

1. Department of MCA, IIMT Meerut U.P. (India)
2. Department of MCA, GKV Haridwar (UK) Pin-249404
3. Disha Institute of Science & Technology, Dhampur U.P. (India)
4. Department of MCA, RKGIT, Ghaziabad U.P. (India) Pin-201003

Abstract: -

The development of Wireless Sensor Networks (WSN) advocates self-organized wireless interconnection of communication devices that would either extend or operate in concert with the wired networking infrastructure or, possibly, evolve to autonomous networks. Unlike traditional wireless networks, WSN do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. One main challenge in design of these networks is their vulnerability to security attacks. Despite the existence of well-known security mechanisms, additional vulnerabilities and features pertinent to this new networking paradigm might render such traditional solutions inapplicable. In particular, the absence of a central authorization facility in an open and distributed communication environment is a major challenge, especially due to the need for cooperative network operation. In *WSN*, any node may compromise the routing protocol functionality by disrupting the route discovery process. In this paper, we understand the various security related issues related to WSN. The security to the network is provided by using cryptographic schemes to build a highly secure framework

Keywords: Cryptography ,Genetic Algorithm ,Wireless Sensor Networks (WSN), Security

Introduction: WSNs are a new paradigm of wireless communication for mobile hosts (which we call nodes). In WSN, there is no fixed infrastructure such as base stations or mobile switching centers. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those that are far apart rely on other nodes to relay messages as routers. Node mobility in an ad hoc network causes frequent changes of the network topology [1,2]. The insecurity of the wireless links, energy constraints, relatively poor physical protection of nodes in a hostile environment, and the vulnerability of statically configured security schemes have been identified as the major challenges. Nevertheless, the single most important feature that differentiates *WSN* is the absence of a fixed infrastructure. No part of the network is dedicated to support individually any specific network functionality, with routing (topology discovery, data forwarding) being the most prominent example. Furthermore, performance issues such as delay constraints on acquiring responses from the assumed infrastructure would pose an additional challenge [3, 4].

1.1 Salient features of the Wireless Sensor Networks (WSN):-

Availability

Availability ensures the survivability of network services despite denial of service attacks. A denial of service attack could be launched at any layer of a WSN. On the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channels**.**

Integrity

Integrity guarantees that a message being transferred is never corrupted. A message could be corrupted because of benign failures, such as radio propagation impairment, or because of malicious attacks on the network.

Confidentiality

Confidentiality [5] ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, such as strategic or tactical military information, requires confidentiality

Authentication

Authentication enables a node to ensure the identity of the peer node it is communicating with. Without authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes.

1.2 Challenges of the features of WSN:

First, use of wireless links renders an ad hoc network susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay, and message distortion. Eavesdropping might give an adversary access to secret information, violating confidentiality. Active attacks might allow the adversary to delete messages, to inject erroneous messages, to modify messages, and to impersonate a node, thus violating availability, integrity, authentication, and non-repudiation. Secondly, nodes, roaming in a hostile environment (e.g., a battlefield) with relatively poor physical protection, have non-negligible probability of being compromised. Therefore, we should not only consider malicious attacks from outside a network, but also take into account the attacks launched from within the network by compromised nodes [6, 7].

2. Secure Routing

To achieve availability, routing protocols should be robust against both dynamically changing topology and malicious attacks. There is no single standard routing protocol. Therefore, we aim to capture the common security threats and to provide guidelines to secure routing protocols. In most routing protocols, routers exchange information on the topology of the network in order to establish routes between nodes. There are two sources of threats to routing protocols. The first comes from external attackers. By injecting erroneous routing information, replaying old routing information, or distorting routing information, an attacker could successfully partition a network or introduce excessive traffic load into the network by causing retransmission and inefficient

routing. The second and also the more severe kind of threats come from compromised nodes, which might advertise incorrect routing information to other nodes.[7, 8] Detection of such incorrect information is difficult: merely requiring routing information to be signed by each node would not work, because compromised nodes are able to generate valid signatures using their private keys. To defend against the first kind of threats, nodes can protect routing information in the same way they protect data traffic, i.e., through the use of cryptographic schemes such as digital signature. However, this defense is ineffective against attacks from compromised servers. Detection of compromised nodes through routing information is also difficult in an ad hoc network because of its dynamically changing topology: when a piece of routing information is found invalid, the information could be generated by a compromised node, or, it could have become invalid as a result of topology changes. It is difficult to distinguish between the two cases. As long as there are sufficiently many correct nodes, the routing protocol should be able to find routes that go around these compromised nodes. Such capability of the routing protocols usually relies on the inherent redundancies multiple, possibly disjoint, routes between nodes in WSN.

The presence of even a small number of adversarial nodes could result in repeatedly compromised routes, and, as a result, the network nodes would have to rely on cycles of time-out and new route discoveries to communicate [9]. This would incur arbitrary delays before the establishment of a non-corrupted path, while successive broadcasts of route requests would impose excessive transmission overhead. The proposed here method combats such types of misbehavior and safeguards the acquisition of topological information. The method describes that a node initiating a route discovery will be able to identify and discard replies providing false topological information, or, avoid receiving them. Moreover, the novelty of the method, as compared with other *WSN* secure routing schemes, is that false route replies, as a result of malicious node behavior, are discarded partially by benign nodes while in-transit towards the querying node, or deemed invalid upon reception. It is to be noted that, the above-mentioned goals are achieved with the existence of a security association between the pair of end nodes only, without the need for intermediate nodes to cryptographically validate control traffic.

3. Scope of Secure Routing

Traditional security mechanisms, such as authentication protocols, digital signature, and encryption, still play important roles in achieving confidentiality, integrity, authentication, and non-repudiation of communication in ad hoc networks.[3, 10] However, these mechanisms are not sufficient by themselves. We take advantage of redundancies in the network topology (i.e., multiple routes between nodes) to achieve availability. In addition to this second principle is distribution of trust. Although no single node is trustworthy in an ad hoc network because of low physical security and availability, the trust is distributed to an aggregation of nodes. It is assumed that any x + 1 node will unlikely be all compromised, consensus of at least x+1 node is noteworthy. Cryptographic techniques are used extensively to provide secure routing. All key-based cryptographic schemes (e.g., digital signature) demand a key management service, which is responsible for keeping track of bindings between keys and nodes and for assisting the establishment of mutual trust and secure communication between nodes. Cryptographic schemes, such as digital signatures, to protect both routing information and data traffic are employed [11]. These schemes usually require a key management service. A public key infrastructure is adopted because of its superiority in distributing keys and in achieving integrity and non-repudiation. Efficient secret key schemes are used to secure further communication after nodes authenticate each other and establish a shared secret session key. In a public key infrastructure, each node has a public/private key pair. Public keys can be distributed to other nodes, while private keys should be kept confidential to individual nodes. A public key should be

revoked if the owner node is no longer trusted or is out of the network; a node may refresh its key pair periodically to reduce the chance of a successful brute-force attack on its private key. We distribute the trust to a set of nodes by letting these nodes share the key management responsibility. The expansion of the electronic information has brought with it a natural demand to make telecommunication systems more open. Systems should become accessible to unknown users who are not regular members of a system's user group. Such users may access systems from remote sites via communication networks. To cope with new conditions like these, strong security mechanism will be required in every telecommunication system. Security is a critical issue in a Wireless Sensor Networks (WSN). As compared with an infra structured or wired network, a WSN poses many new challenges in security. For example, wireless channel is more vulnerable to attacks such as passive eavesdropping or active signal inference and jamming; the co-operative WSN protocols are more vulnerable to denial of service attacks; the lack of infrastructure and limited resources restrict the applicability of some conventional security solutions; and the un-predictable ad hoc mobility makes it more difficult to detect the malicious behavior. Due to these new challenges many security solutions that have been effective in a wired network become inapplicable in a WSN. Much effort has been made to develop applicable security solutions dedicated to a WSN environment. Among them, key management probably the most critical and development security issue in a WSN, has attracted much attention [12]. A number of secure routing protocols have also been proposed to protect the correctness of different types of ad hoc networking protocols, both table- driven/on-demand and distance vector. Data confidentiality is the protection of transmitted data from passive attacks, such as eavesdropping. Sensitive information, such as tactical military information transmitted across a battlefield requires confidentiality Leakage of such information to enemies could result into devastating consequences [13, 14]. Messages transmitted over the air can be eavesdropped from anywhere without having the physical access to the network components. Conventionally confidentiality is achieved by cryptography [15]. However the limited sources, such as the limited power battery and processing capability restrict the use of computationally intensive encryption schemes in a WSN. The computationally efficient encryption is schemes sometimes are not secure enough. A more severe problem in WSN is that, mobile nodes usually reside in an open and hostile environment [16, 17, and 18]. Nodes themselves might be compromised. For example, in the battle field scenario nodes might be captured. In this case all the credential stored in the nodes would be compromised, including the keys. Any encryption scheme no matter how secure it is would not help. Based on these observations a novel scheme is proposed to statistically enhance data confidentiality in a WSN. Assume that we have a secret message, if we send it through a single path; the enemy could compromise it by compromising any one of the nodes along the path. However if we divide it into multiple pieces, and send the multiple pieces via multiple independent paths, then the enemy would have to compromise all the pieces from all the paths to compromise the message. Improved security can be achieved by this means [19]. Thus by spreading the traffic onto multiple paths, it also makes it harder for the enemy to decrypt the message.

4. Problem Formulation

The main objective of this work is to select an optimized route among the defined zones and each zone having certain number nodes. Once the optimized route is selected with its respective cost function (high throughput route), the message is sent through the route using cipher encryption. In this case the message is divided into various packets (letters) and then it is (encrypted message) transmitted through the selected route. On the receiver side each letter is decrypted according to the agent code and the original message is retrieved. In this, we have taken up a WSN between two places on a map and have divided the region into

various zones consisting in each region, so as to standardize input data for normalization. After that we have taken up the shortest path as the backbone and assigned it the highest priority. In order to achieve the desired result the algorithms of Analytical Hierarchy Process, Genetic Algorithm and Encryption is used.

5. Analytical Hierarchy Process

The analytical hierarchy process performs three fundamental procedures:

1. Preferences for different alternatives depend on separate criteria which can be reasoned about independently and given numerical scores.

2. The score from a given criteria can be calculated from sub criteria. That is, the criteria can be calculated in a hierarchy, and the score at each level of hierarchy can be calculated as a weighted sum of the lower level scores.

3. At a given level, suitable scores can be calculated from only pair wise comparisons

Genetic Algorithm:

The steps involved in genetic algorithm are as follows -

1. [Start] Generate random population of n chromosomes (suitable solutions for the problem)

2. [Fitness] Evaluate the fitness f (x) of each chromosome x in the population

3. [New population] create a new population by repeating following steps until the new population is complete

a. [Selection] Select two parent chromosomes from a population according to their fitness (the better fitness, the bigger chance to be selected)

b. [Crossover] With a crossover probability cross-over the parents to form new offspring (children). If no crossover was performed, offspring is the exact copy of parents.

c. [Mutation] with a mutation probability mutates new offspring at each locus (position in chromosome).

d. [Accepting] Place new offspring in the new population

e. [Replace] Use new generated population for a further run of the algorithm.

f. [Test] if the end condition is satisfied, stops, and returns the best solution in current population.

4. [Loop] Go to step 2

Encryption Algorithm:

Following are steps involved in encryption –

a. Enter the agent key which will decide the encryption pattern of the message at the transmitting side.

b. Once the agent key is entered, the message is passed to the transmitting end which gets encrypted according to the agent key (cipher encryption). This sort of encryption is safe from brute force attack as the message gets randomly shuffled infinite no of times which makes the information more secure.

c. Once each of the packet reaches to the receiving side it gets decrypted and the original message is received.

6. Simulation & Discussions

The simulation is done for various zones (the user defines the number of zones) and the optimized routing is determined by the value of cost function. The optimized route is selected with the use of analytical hierarchy process and genetic algorithm. Once the optimized route is selected the encryption algorithm is applied to make the routing secure.

Cost Function = B1x1+ B2x2 + B3x3+B4x4 (1)

The values of various local constraints are as follows (for an area having three zones):-

B1= 0.35

B2= 0.25

B3= 0.30

B4=0.10

For the transfer of the first alphabet of the message the optimized path is to be decided with the help of analytical hierarchy process and genetic algorithm. For our purpose 4 zones are taken with each zone consisting of 4 nodes, in total there are 256 values.

With the help of the comparison matrix and AHP various values are put in the table. The attributes which are considered for the route are latency, node status and power consumption. These are the attributes which determine the cost function values and also act as an input to genetic algorithm simulator. For example

For zone 1(Z1):-

Node 1(N1):-

Comparison matrix for Z1 N1

Attributes	Latency	Power Consumption	Node Status
Latency	1	2	4
Power Consumption	0.1	1	4
Node Status	0.25	0.25	1

Cost function 1 = 35

Node 2(N2):-

Comparison matrix for Z1 N2

Attributes	Latency	Power Consumption	Node Status
Latency	1	4	6
Power Consumption	0.25	1	2
Node Status	0.16	0.5	1

Cost function 2 = 39

Node 3(N3):-

Comparison matrix for Z1 N3

Attributes	Latency	Power Consumption	Node Status
Latency	1	6	8
Power Consumption	0.16	1	4
Node Status	0.125	0.25	1

Cost function 3= 40

Node 4(N4):-

Comparison matrix for Z1 N4

Attributes	Latency	Power Consumption	Node Status
Latency	1	4	6
Power Consumption	0.25	1	4
Node Status	0.16	0.25	1

Cost function 4= 38

After the cost functions values are obtained they are converted to binary values and the genetic algorithm is run through those values in terms of crossover and mutation. Once the optimized cost function values are obtained, we know the path through which the message is sent. The encryption and cryptography algorithm is applied in order to make the route secure. What have seen in going through paper of various Wireless Sensor Networks routing algorithms, various routing protocols such as (proactive and reactive) by taking into consideration various communication parameters tend to give throughput gain (efficiency) in range of 30%-50%. It has been proposed that the route optimization using GA and AHP (First time in packet technology network) results in greater saving of power (taking power consumption as the backbone). In this case, AHP is being used for the selection of the performance indices depending on various linguistic variables in different time zones. If consider that the probability of passing information is 33.33% for a certain instance using GA (i.e. no. of iterations required to pass on the information through a particular node/frequency of the node. The frequency of node refers to the no of times the same node is being passed for passing the information. Here for calculation purpose the frequency of node is taken as 10. If the probability of passing information through a node is less than 50% then the power saved by the node is in the range of 70-80%.The node selection (and finally route optimization) depends upon the function or objective function. The objective function further depends upon the application used. Simulation results using GA and AHP along with cipher encryption show an average throughput gain (where throughput gain is the amount of information passing from input to output) of 55% to 75%, depending on network density, over traditional minimum hop route selection in 802.11b networks. Also in this case the message is more secure as the message is encrypted and sent through the optimize route. If the traffic patterns are not clear in a large network, even an optimal routing algorithm will achieve low throughput. Each region is being characterized by three nodes (as evident from the nine cost functions) where every node has in turn four parameters (Traffic Congestion, Node density, node status,

power consumption), which are key to any communication problem. The definition of realistic mobility models is one of the most critical and, at the same time, difficult aspects of the simulations of applications and systems designed for mobile environments. Currently, there is no publicly available data capturing node movement in real large-scale WSN environments. Taken together, for those systems in which mobility is important and for which a synthetic mobility model is an essential ingredient, it would appear to be important to consider the influence of the human-level social network as something that informs likely individual and group mobility patterns. The traditional technique used by most existing ad hoc routing protocols is to select minimum hop paths. These paths tend to contain long-range links that have low effective throughput and reduced reliability. It should be possible to enhance the multi-rate network performance of almost any existing shortest path based protocol by adapting it to use in our medium time metric system. A greater reduction in effective throughput for faster links is observed because the time necessary to send a packet is inversely proportional to the rate of link. In other words, the data transmission time is small for fast links; the proportion of time consumed by the fixed overhead is large. In multi-rate wireless networks, the selection of minimum hop paths typically results in the links operating at low rates. The following curves show the improvement in the efficiency of the proposed and existing algorithm with the attributes of the route and also securing the network.

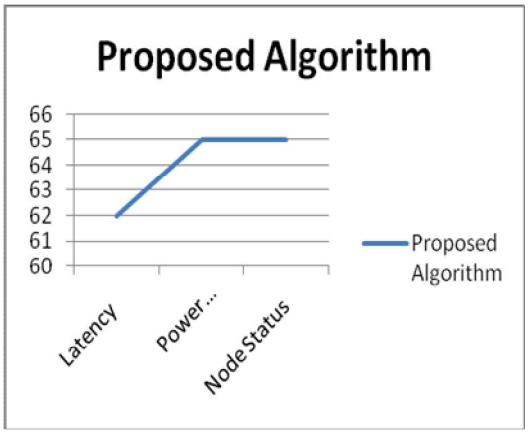

Figure 1 Represents the proposed algorithm for securing WSNs.

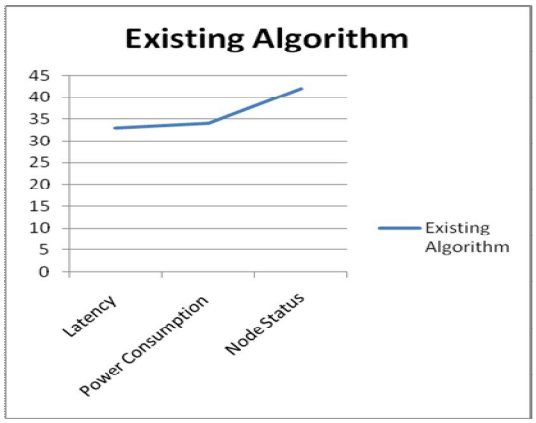

Figure 2 Represents the existing algorithm for securing WSNs.

7. Conclusion

The application of intelligent techniques in combination with the mathematical tools such as AHP brings a pronounced throughput improvement in WSN. The route is also secure by using cipher encryption. To build a highly available and highly secure key management service, the use of cipher cryptography is proposed to distribute trust among a set of nodes. Our encryption technique service employs share refreshing to achieve proactive security and to adapt to changes in the network in a scalable way. Finally, by relaxing the cost functions attributes requirement on the nodes, our service does not rely on synchrony assumptions. Such assumptions could lead to vulnerability. A prototype of the key management service has been implemented, which shows its feasibility. By using GA and AHP for routing, the WSN throughput has shown an improvement of in comparison to the existing routing algorithms. The proposed model is relatively simple (using GA and AHP), but is parameterisable in a way that allows different scenarios to be modeled both at the level of social organization and topographical translation.

REFERENCES

[1] M. J. Neely. *Dynamic Power Allocation and Routing for Satellite and Wireless Networks with Time Varying Channels.* PhD thesis, Massachusetts Institute of Technology, LIDS, 2003.

[2] M. J. Neely and E. Modiano." Capacity and delay tradeoffs for ad-hoc mobile networks". (Invited Paper) IEEE BroadNets, San Jose, CA, Oct. 2004.

[3] R.L. Cruz and A. V. Santhanam." Hierarchical link scheduling and power control in multihop wireless networks." Proceedings of the 40th Annual Allerton Conference on Communication, Control, and Computing, Oct.2002.

[4] M. J. Neely, E. Modiano, and C. E Rohrs. "Dynamic power allocation and routing for time varying wireless networks". IEEE Journal on Selected. Areas in Communications, January 2005.

[5] M. Grossglauser and D. Tse. "Mobility increases the capacity of ad-hoc wireless networks". Proceedings of IEEE INFOCOM, 2001.

[6] P. Gupta and P.R. Kumar. *The capacity of wireless networks.* IEEE Transactions on Information Theory, vol. 46, no. 2:pp. 388–404, March2000.

[7] N. Bansal and Z. Liu. "Capacity, delay and mobility in wireless ad-hoc networks". IEEE Proceedings of INFOCOM, April 2003.

[8] M. Grossglauser and M. Vetterli. "Locating nodes with ease: Last encounter routing in ad hoc networks through mobility diffusion". IEEE Proceedings of INFOCOM, April 2003.

[9] Bruce Schneier. *Secrets and Lies. Digital Security in a Networked World*. John Wiley $ Sons, Inc, 1st edition, 2000.

[10] Bradley R. Smith, Shree Murthy, and J.J. Garcia-Luna-Aceves. "Securing distance-vector routing protocols." In Proceedings of Internet Society Symposium on Network and Distributed System Security, San Diego, CA, pages 85–92, February 1997.

[11] Po-Wah Yau and Chris J. Mitchell. "Reputation methods for routing security for mobile ad hoc networks." In Joint IST Workshop on Mobile Future and Symposium on Trends in Communications (SympoTIC '03), Bratislava, Slovakia, October 2003.

[12] Seung Yi, Prasad Naldurg, and Robin Kravets. "Security-aware ad-hoc routing for wireless networks". MobiHOC Poster Session, 2001.

[13] Bin Yu and Munindar P. Singh. "Detecting deception in reputation management". In Proceedings of Second International Joint Conference on Autonomous. Agents and Multi-Agent Systems, pages 73–80, 2003.

[14] Yongguang Zhang and Wenke Lee. "Intrusion detection in wireless ad-hoc networks." In Proceedings of MOBICOM 2000, pages 275–283, 2000.

[15] Yongguang Zhang and Wei Li. "An integrated environment for testing mobile ad-hoc networks." In Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne, CH, June 2002. IEEE.

[16] S. Zhong, Y. Yang, and J. Chen. Sprite: "A simple, cheat-proof, credit-based system for mobile ad hoc networks". Proceedings of Infocom, 2003.

[17] Lidong Zhou and Sigmund Haas. *Securing ad hoc networks.* In *IEEE* Network magazine, special issue on networking security, Vol. 13, No. 6, November/December, pages 24–30, 1999.

[18] L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks" Proc. of the ACM Conference on Computer and Communications Security, Washington D.C., November 2002, pp. 41-47.

[19] V.D. Gligor and S. I. Gavrila, *Application-Oriented Security Policies and Their Composition*, in Security Protocols, B. Christianson, B. Crispo, M.Roe (eds.), Lecture Notes in Computer Science 1550, Springer Verlag, 1999, pp. 67-75.

[20] V. D. Gligor, H. Khurana, R. K. Koleva, V. G. Bharadwaj, and J. S. Baras. *On the negotiation of access control policies.* In B. Christianson et al., editors, Security Protocols in Lecture Notes in Computer Science, vol. 2467, pp. 188–201, Springer Verlag, 2002. Also see transcript of discussion, pp. 202-212.