ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 4, April 2019

Modified ACO Cluster based Key Management Routing Mechanism for WSN Security

B.Vaishnavi [1], Mrs. C.P.Gowthami M.E.,[2]

P.G. Student, Department of ECE, GRT Institute of Engineering and Technology, Tiruvallur, Tamil Nadu, India [1]

Assistant Professor, Department of ECE, GRT Institute of Engineering and Technology, Tiruvallur, Tamil Nadu, India [2]

ABSTRACT: The security of wireless sensor network is becoming more and more important, in which key management is an important part to realize the security of the networks. In the hierarchical network, cluster heads play an important role in the network. Once being captured, they will expose more keys and information. Therefore, how to choose the cluster head should be considered seriously. This paper presents a new sophisticated collusion attack scenario against a number of existing IF algorithms based on the false data injection. In such an attack scenario, colluders attempt to skew the aggregate value by forcing such IF algorithms to converge to skewed values provided by one of the attackers. However, the existing clustering algorithms only consider energy factor when selecting cluster heads. The data aggregation process make the wireless sensor network is vulnerable to wormhole attack. This work proposes the distributed wormhole attacker detection mechanism that improves the detection accuracy using iteration filtering mechanism. Providing initial approximation to the sensor nodes' trustworthiness makes the proposed algorithm as collusion robust with faster converging.

KEYWORDS: WSN Security, ACO, Attacks.

I. INTRODUCTION

The security of wireless sensor network is becoming more and more important, in which key management is an important part to realize the security of the networks. In the hierarchical network, cluster heads play an important role in the network. Once being captured, they will expose more keys and information. Therefore, how to choose the cluster head should be considered seriously. However, the existing clustering algorithms only consider energy factor when selecting cluster heads. This paper proposes a model regarding probability of nodes being captured which not only considers the energy factors, but also considers the nodes capture probability when choosing cluster heads, so that nodes which hold smaller capture probability tend to be the cluster heads. On the basis of this model, an efficient key agreement scheme is proposed, which can use EBS (Exclusion Basis Systems) structure to update the group keys between clusters effectively. Simulation experiments show the proposed scheme has good connectivity and node capture resistance, and it can also save more storage cost.

II. RELATED WORK

1) **Wireless Network Design for Control Systems: A Survey** Pangun Park ; Sinem Coleri Ergen ; Carlo Fischione ; Chenyang Lu ; Karl Henrik Johansson

Wireless networked control systems (WNCSs) are composed of spatially distributed sensors, actuators, and controllers communicating through wireless networks instead of conventional point-to-point wired connections. Due to their main benefits in the reduction of deployment and maintenance costs, large flexibility and possible enhancement of safety, WNCS are becoming a fundamental infrastructure technology for critical control systems in automotive electrical systems, avionics control systems, building management systems, and

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 4, April 2019

industrial automation systems. The main challenge in WNCS is to jointly design the communication and control systems considering their tight interaction to improve the control performance and the network lifetime.

2) **Comparative analysis of wireless sensor networks with wireless multimedia sensor networks -** Ahmed Mateen ; Maida Sehar ; Khizar Abbas ; Muhammad Azeem Akbar

In this paper, we provide Survey on comparison of different protocol of Wireless sensor network and wirelesss multimedia sensor network like Greedy Perimeter Stateless Routing for Wireless Networks (GPSR), Real-time and Energy Aware Qos routing protocol (REAR), Temporary ordered routing Algorithm (TORA) and Dynamic source routing (DSR). These different protocols with WMSN are compared in requisites of throughput, end-to-end delay, network life time.

3) **Proficient key management scheme for multicast groups using group key agreement and broadcast encryption**-E. Abirami ; T. Padmavathy

Key Management techniques are exercised to distribute and update keys such that illegitimate parties cannot ingress group communications. Key management, however can exhibit information about the stream of group association, such as group size and the number of joining and leaving users. This is a threat to applications with confidential group membership information. This project proposes a new key management paradigm which a combination of traditional broadcast encryption and group key agreement which never reveals the group dynamic information to outsiders and achieves both forward secrecy and backward secrecy.

4) **A Survey of Recent Achievements for Wireless Sensor Networks Testbeds -** Junyan Ma ; Jin Wang ; Te Zhang

Wireless sensor networks (WSNs) are widely used in the area of military, industrial, environmental monitoring and marine exploration applications. The applications are, however, prone to unexpected problems or failure during post deployment. This is mainly due to the limited testing of applications in pre-deployment tests. Testbeds are commonly used for analyzing performance and uncovering potential problems of sensor network applications in pre-deployment tests.

5) **An improved K-means cluster-based routing scheme for wireless sensor networks -** Mohamed Lehsaini ; Meriem Bouchra Benmahdi

In this paper, we propose two cluster-based routing schemes. The first is based on K-means approach and the second is an improved version of K-means approach. The latter generates balanced clusters, which allows to distribute the load equitably among the cluster-heads. Simulation results show that the proposed routing schemes balance the energy consumption among the cluster-heads, and significantly improves the network lifetime compared to LEACH (Low Energy Adaptive Clustering Hierarchy) protocol.

6) **An energy aware dynamic cluster head selection mechanism for wireless sensor networks-** Maryam Kalantari ; Gholamhossein Ekbatanifard

In this paper, a protocol has been proposed to select the sensor node as cluster head, in the sense that choosing the closest sensor node to low-energy nodes will result in lesser energy consumption and early death prevention of nodes. The simulation results have been shown that the proposed protocol could enhance the network lifetime.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 4, April 2019

III. PROPOSED ALGORITHM

EXISTING METHODOLOGY

PSO algorithm is an iterative optimization algorithm, which initializes the particle swarm into a set of random solutions, and all particles follow the current optimal particle to search the optimal solution in the solution space. During the iteration, the particles are updated according to 2 extremums, namely their own individual extremum and global extremum. Among them, the individual extremum is the optimal solution found by the particle, and the global extremum is the optimal solution found by the entire particle swarm. In computational science, particle swarm optimization (PSO) is a computational method that optimizes a problem by iteratively trying to improve a candidate solution with regard to a given measure of quality. It solves a problem by having a population of candidate solutions, here dubbed particles, and moving these particles around in the search-space according to simple mathematical formulae over the particle's position and velocity. Each particle's movement is influenced by its local best known position, but is also guided toward the best known positions in the search-space, which are updated as better positions are found by other particles. This is expected to move the swarm toward the best solutions PSO shares many similarities with evolutionary computation techniques such as Genetic Algorithms (GA). The system is initialized with a population of random solutions and searches for optima by updating generations. However, unlike GA, PSO has no evolution operators such as crossover and mutation. In PSO, the potential solutions, called particles, fly through the problem space by following the current optimum particles. The detailed information will be given in following sections.

Disadvantages

- The disadvantages of particle swarm optimization (PSO) algorithm are that it is easy to fall into local optimum in high-dimensional space and has a low convergence rate in the iterative process.
- The method easily suffers from the partial optimism, which causes the less exact at the regulation of its speed and the direction.
- The method cannot work out the problems of non-coordinate system, such as the solution to the energy field and the moving rules of the particles in the energy field

PROPOSED METHODOLOGY

In computer science and operations research, the ant colony optimization algorithm (ACO) is a probabilistic technique for solving computational problems which can be reduced to finding good paths through graphs. Artificial Ants stand for multi-agent methods inspired by the behaviour of real ants. The pheromone-based communication of biological ants is often the predominant paradigm used. Combinations of Artificial Ants and local search algorithms have become a method of choice for numerous optimization tasks involving some sort of graph, e. g., vehicle routing and internet routing. The burgeoning activity in this field has led to conferences dedicated solely to Artificial Ants, and to numerous commercial applications by specialized companies such as Ant Optima. As an example, Ant colony optimization is a class of optimization algorithms modeled on the actions of an ant colony. Artificial 'ants' (e.g. simulation agents) locate optimal solutions by moving through a parameter space representing all possible solutions. Real ants lay down pheromones directing each other to resources while exploring their environment. The simulated 'ants' similarly record their positions and the quality of their solutions, so that in later simulation iterations more ants locate better solutions. One variation on this approach is the bees algorithm, which is more analogous to the foraging patterns of the honey bee, another social insect.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 4, April 2019

Advantages

- Relatively efficient.
- Performs better against other global optimization techniques such as Neural net, genetic algorithms, simulated annealing.
- Can be used in dynamic applications.
- Convergence is guaranteed, but time to convergence uncertain

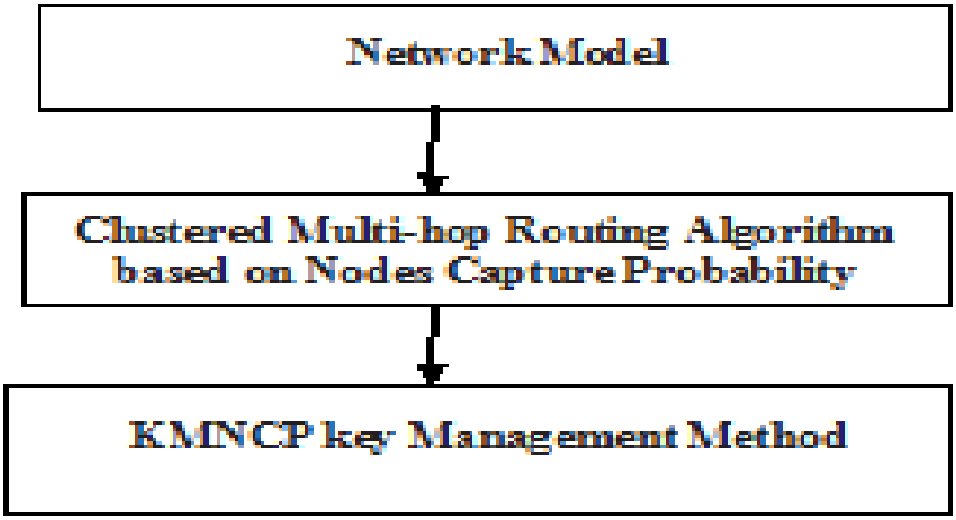

Figure 3.1 Flow diagram of the Proposed Sytem.

ANT COLONY OPTIMIZATION

Ants update the level of pheromone while they are constructing their schedules by iteratively adding new sessions to the current partial schedule. At each time step, ants compute a set of feasible moves and select the best one according to some probabilistic rules based on the heuristic information and pheromone level. The higher value of the pheromone and the heuristic information, the more profitable is to select this move and resume the search. The selected node is putted in the tabu list related to the ant to prevent to be chosen again. Heuristic information represents the nearer sessions around the current session, while pheromone level "memory" of each path represents the usability of this path in the past to find good schedules. At the end of each iteration, the tabu list for each ant will be full and the obtained cheapest schedule is computed and memorized. For the following iteration, tabu lists will be emptied ready for use and the pheromone level will be updated. This process is repeated till the number of iterations (stopping criteria) has been reached.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 4, April 2019

IV. RESULTS AND DISCUSSIONS

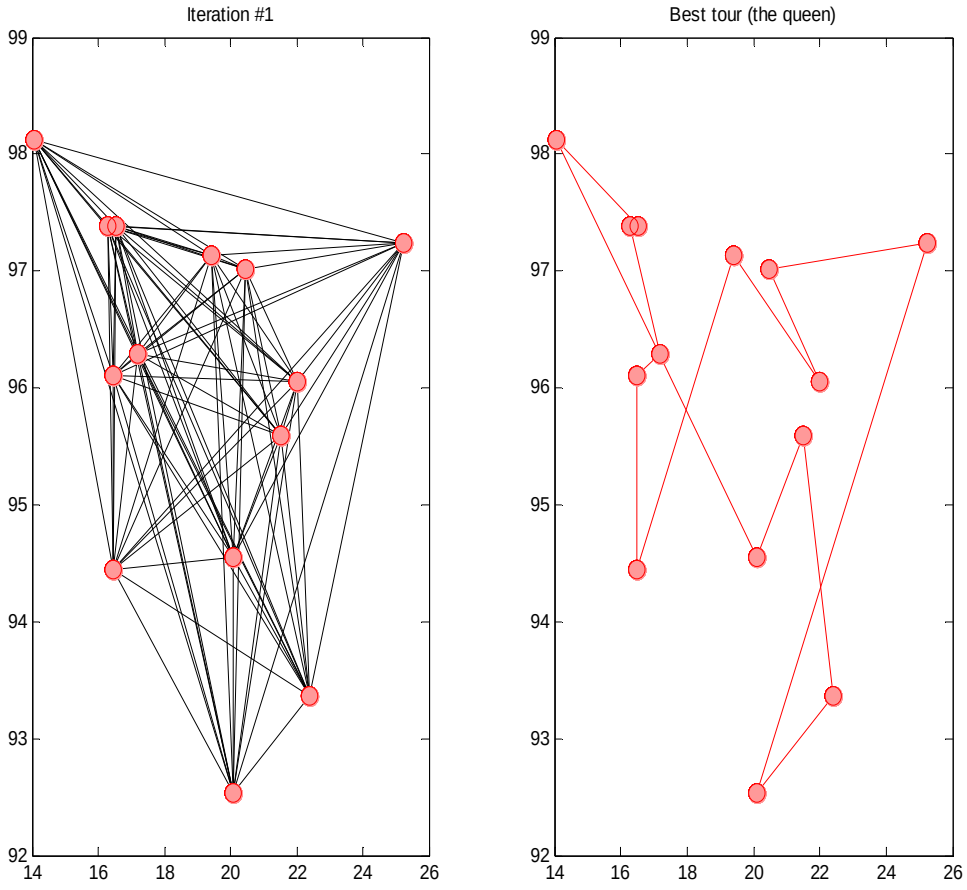

Figure 4.1 Nodes Distribution

The above figure represents the node clustered distribution in left figure and with secure key transfer routing takes place in the right figure. Initially the clusters will take the entire path and secondly the main path is selected using key management Ant Colony Optimization.

V. CONCLUSION AND FUTURE WORK

Ant colony algorithm, which is used to deceive the intruders in the path planning initialization can also improve and safeguard the data collection from the base station to the nodes and vice versa. The idea is to allow the non-uniform distribution of KMT with the initial pheromone and the selection strategy with direction playing a very positive role in the path search. This method will deceive the intruders while introducing the actual coverage and updating strategy of pheromone repeatedly in false search and eliminating the effect of the intruders. In addition, the pheromone disappearance coefficient is segmented and adjusted, which can effectively balance the convergence speed and communication of the sensor nodes. Finally, this research provides a theoretical basis for key management

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 4, April 2019

technique with an ant colony optimization by strict mathematical derivation, and some numerical evaluations using MATLAB

REFERENCES

1. J Yick, B Mukherjee, D Ghosal, "Wireless sensor network survey", Computer networks, vol. 52, no. 12, pp. 2292-2330, 2008.
2. S Waware, DN Sarwade, P. Gangurde, "A review of power efficient hierarchical routing protocols in wireless sensor networks", International Journal of Engineering Research and Applications, vol. 2, no. 2, pp. 1096-1102, 2012.
3. SA Camtepe, B. Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks", Computer Security-ESORICS 2004, pp. 293-308, 2004.
4. Y Xiao, VK Rayi, B Sun et al., "A survey of key management schemes in wireless sensor networks", Computer communications, vol. 30, no. 11, pp. 2314-2341, 2007.
5. G Jolly, MC Kuscu, P Kokate et al., "A low-energy key management protocol for wireless sensor network", Proc. of the Eighth IEEE Intl. Symposium on computers and communication (ISCC'03), pp. 335-340, 2–3 July, 2003.
6. Sencun Zhu, S. Sanjeev, J. Sushi, "LEAP: efficient security mechanisms for Large-scale distributed sensor networks", proceedings of the 10th ACM Conference on Computer and Communication Security, pp. 62-72, 2003.
7. X Du, Y Xiao, M Guizani et al., "An effective key management scheme for heterogeneous sensor networks", Ad Hoc Networks, vol. 5, no. 1, pp. 24-34, 2007.
8. M Eltoweissy, MH Heydari, L Morales et al., "Combinatorial optimization of group key management", Journal of Network and Systems Management, vol. 12, no. 1, pp. 33-50, 2004.
9. M Younis, K Ghumman, M. Eltoweissy, "Location-aware combinatorial key management scheme for clustered sensor networks", IEEE Transactions on Parallel and Distributed Systems, vol. 17, no. 8, pp. 865-882, 2006.
10. M. Clerc, J. Kennedy, "The particle swarm: Explosion stability and convergence in a multi-dimensional complex space", IEEE Transactions on Evolutionary Computation, vol. 6, pp. 58-73, 2002.
11. N. Xu, "A survey of sensor network applications", IEEE Communications Magazine, vol. 40, no. 8, pp. 102-114, 2002.