ISSN 2249-6343
International Journal of Computer Technology and Electronics Engineering (IJCTEE)
Volume 2, Issue 1

Novel Probabilistic Approach for Detecting Attack on Routing Protocols in Wireless Sensor Network

Ravindra Gupta, Hema Dhadhal

Abstract: **The proposed system come up with an idea for detecting various types of routing attacks in wireless sensor network considering AODV protocol. Considering the previous research work , system identifies the probability of the routing attack over the dynamic topology of wireless sensor network where it has assumed a faster propagation of the infection towards the nodes. To ensure the success in mitigating the attacks the proposed model make use of an adversary module which works either on node attack or link or route attack form. The proposed is different from existing one because it tries to cover all types of attacks. The system make use of probabilistic approach for modelling the routing attack scenario over WSN. The uniqueness is that majority of the prior research work has focused on one type of routing attack, whereas the proposed system is making use of one or more type of sequential attacks. The simulation results show highly contrastive result when compared with frequently used current algorithm for mitigating routing attacks.**

Index Terms - Routing Attack, Wireless Sensor Network, Security, AODV, Probabilistic approach

I. INTRODUCTION

Constant research has been done in wireless sensor network for security issues which normally consists of independent wireless sensor nodes which group together to form a momentary wireless network without any assistance of any centralized management or fixed infrastructure. Routing protocols are normally required for maintaining efficient transmission among the mobile nodes by exploring the network topology, which in this case is always dynamic. It also designs a route for pushing the data packets and also manages the routes among the pair of mobile nodes. One of the fundamental problem with majority of the routing protocol is that the routing protocol relies on all the mobile nodes present in the network and depending on the situation that these mobile nodes will perform or collaborate appropriately; but there is a higher feasibility of circumstances where certain specific set of nodes may not behave appropriately giving rise to suspicious factor.

Unfortunately, majority of the routing protocols in wireless sensor network is witnessed for declined performance at the time of communicating with large scale of misbehaving nodes, which definitely sustains the course of route exploration but also disrupt the course of data rendering the routing protocol to resume again the route exploration procedure or to chose an unconventional route in case it is available. Moreover the newly opted route has the feasibility of possessing a few malicious nodes, resulting in failure of new route too. The fundamental issue with frequently used routing protocols is that they rely all mobile nodes of network and based on the assumption that nodes will behave or cooperate properly but there might be a condition where some nodes are not behaving properly. Majority of the adhoc network routing protocols becomes inefficient and shows reduced performance while mitigating with big number of misbehaving nodes. Such set of misbehaving nodes support the flow of route discovery traffic but interrupt the data flow, causing the routing protocol to restart the route-discovery process or to select an alternative route if one is available.

The proposed paper will present a framework for mitigating majority of the types of routing attack using probabilistic approach. The proposed system has large dimension of testing conducted to check the efficiency of routing protocol using AODV on majority of routing attack in wireless sensor network. In Section II, we will discuss about the previous research work in this area followed by Section III highlights proposed system followed by conclusion in section IV.

II. RELATED WORK

Considering the dynamic mobility of wireless sensor network we have studied previous research work which focuses on security issues in Mobile Ad-hoc Networks. So in this section we will consider the work done in MANET and its respecting routing protocol. MANET is very much popular due to the fact that these networks are dynamic, infrastructure less and scalable. Despite the fact of popularity of MANET, these networks are very much exposed to attacks [9, 23].

Wireless links also makes the MANET more susceptible to attacks which make it easier for the attacker to go inside the network and get access to the ongoing communication [9, 21]. Different kinds of attacks have been analyzed in MANET and their affect on the network. Attack such as gray hole, where the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior [14]. MANETs routing protocols are also being exploited by the attackers in the form of flooding attack, which is done by the attacker either by using RREQ or data flooding [16]. In any network, the sender wants its data to be sent as soon as possible in a secure and fast way, many attackers advertise themselves to have the shortest and high bandwidth available for the transmission such as in wormhole attack, and the attacker gets themselves in strong strategic location in the network. They make the use of their location i.e. they have shortest path between the nodes [12, 17].

One of the most arising issues in MANET is the limited battery, attackers take an advantage of this flaw and tries to keep the nodes awake until all its energy is lost and the node go into permanent sleep [18]. Many other attacks MANET such as jellyfish attack, modification attack, misrouting attack and Routing Table Overflow have been studied and exposed [19, 13, 20]. In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [21, 22].

This paper focuses on the study the impact of Black Hole attack in MANET using both Reactive and Proactive protocols and to compare the vulnerability of both these protocols against the attack. So this section will consider all the work done towards securitizing mobile adhoc network and its respective routing protocol. Recently, numerous approaches have been proposed to deal with the node non-cooperation problem in wireless networks. They generally can be classified into two main categories: reputation systems and price-based systems. We use a monitoring and reputation system [2] as the basic setting for regular nodes. Many related works also use reputation systems [3]–[5] and a game theory model [6] to analyze the problem. Some recent works have studied the incentives for malicious nodes and modeled their behavior more rationally. In [7], Liu et al. present a general incentive-based method to model the attackers' intents, objectives, and strategies. In [8], Theodorakopoulos and Baras further study the payoff of the malicious nodes and identify the influence of the network topology. However, the good nodes' behavior in [9] is simple, and it fails to consider the possibility that an attacker might choose different attack frequencies toward different opponents.

The security problem and the misbehaviour problem of wireless networks including MANETs have been studied by many researchers e.g. [9], [10], [11], [12].Various techniques have been proposed to prevent selfishness in MANETs. These schemes can be broadly classified into two categories: credit-based schemes and reputation based schemes. The basic idea of credit-based schemes is to provide incentives for nodes to faithfully perform networking functions. Nodes get paid for providing services to other nodes. When they request other nodes to help them for packet forwarding, they use the same payment system to pay for such services.

Depending of the patterns of the intrusion, attacks towards mobile adhoc network can be categorized into active or passive attack. Not only this, the attacks can be also further classified into internal or external attack. In association with the victim node, the attack can be again classified into routing packet or data packet attacks. In case of routing packet attack, the malicious node resist existing routes[13], [14], [15], [16] from being utilized and also it spoofs other non-existing routes for alluring data packets [17], [18], [19], [20] to be forwarded to them.

Although there are number of research conducted in past [21], [22], [23], [24], [25] for analyzing routing attacks on mobile adhoc network. Important routing attacks are fabrication, blackhole, and alteration of various fields in routing packets e.g. RREQ, RREP, RERR message, etc. Research work conducted in [26], [27], [28] discusses about some mitigating techniques for safeguarding the routing protocols in mobile adhoc network. Although these set of research work can successfully resist illegitimate nodes from participating the network, but unfortunately, it was found to increase the significant network overhead with respect to key exchange as well as authentication with restricted intrusion eradication.

The resistance based approach are also found less efficient for mitigation from malicious intruders who already have the confidential information for rendering communication by themselves in the mobile adhoc network. The prior research work has also seen the introduction of Intrusion Detection System for mobile adhoc network.

Unfortunately, due to the dynamic topology of mobile adhoc network, majority of such research work are modeled to be scattered and possesses cooperative data-structure.

Specification-based approaches, for example DEMEM [29], C. Tseng et al. [30] and M. Wang et al. [31], monitor network activities and compare them with known attack features, which are impractical to cope with new attacks. A completely new work done in same field called as Intrusion Response System in mobile adhoc network has being discussed in [32] which detaches the malicious node, once identified, depending on their reputation system. Unfortunately, the work fails to be at par with efficient IDS system.

III. Proposed System

The proposed system presents a framework for contrastive analyzation of routing protocols where the routing attacks can be determined. Majority of the prior research work has focused on building either a mathematical model or any analytical model considering one of the type of routing attack in wireless sensor network. The problem with such approach is that it can better thwart for one of the routing attack while become inefficient for other types of routing attack. So, due to this research gap, the proposed system has focused on designing a hybrid framework which can model almost all types of routing attack in wireless sensor network thereby acting as an effective solution for identifying the sectors of routes which are compromised or about to be compromised.

The proposed system can be classified into following modules e.g. network model, cryptographic model, attacker model.

A. Network Model:

The current work of mechanizing the security in routing protocol is designed considering group of nodes N and routes R, which can be represented mathematically as G={N, R}as directed graph. The route R is completely dependent on factors like current position of node, relationship, and charecteristics of the mobile nodes, medium of communication, and MAC layer. The dispatcher and destined nodes can be depicted as D and d, which is constructed depending on decision taken by routing protocol. One or multiple routes will be designed considering set of sequential R for a given set of dispatcher node D and destined node d. Cumulative route $CR_{D,d}$ is designed for all the links considered from D to d. Let F_t signifies the part of the travel from D to d such that it travels the path $t \epsilon CR_{Dd}$. The cumulative route CR_{Dd} can be depicted as route sub-graph G_{Dd} of G possessing mobile nodes and directed graph travelled by atleast one of the routes $t \epsilon CR_{Dd}$. The routing protocol using AODV is designed based on segregating the spatial factors depending on packets forwarded along the diversified routes. The consideration is made for both single and multi-paths.

B. Cryptographic Model:

The module will be responsible for maintaining security of the packets by assigning cryptographic keys. The model considers S_{key} as group of symmetric security keys and P_{key} be equivalent group of public keys. If i be node number considered than $i \epsilon N$, which is allocated with S'_{key} such that $S'_{key} \subseteq S_{key}$ and also public tag substitution key $P'_{key} \subseteq P_{key.}$ The common set of the keys shared among i and j as $S_{key(i,\ j)} = S_{key(i)} \cap S_{key(j)}$, which is the criteria for permitting transmission of packets between i and j when $S_{key(i, j)} \neq 0$. The representation is as shown in Fig.1. It is also considered that the model will use $S_{key(i, j)}$ shared keys completely in order to protect the specified route (i, j). Therefore, the proposed model should have some common keys in $S_{key(i, j)}$ for secure communication in specified route. Not only this, the model will also consider the computation of $P_{key(i, j)}$ as $P_{key}(i) \cap P_{key(j)}$ for the purpose of estimating the group of shared key $S_{key(i, j)}$.

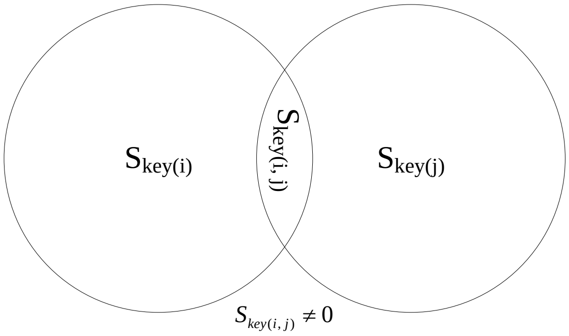

Fig.1. Set Representation of Cryptographic assumption

The category of public tag substitution design will posses any rule which facilitates required data from any other mobile nodes $j \epsilon N$ in order to evaluate group of $P_{key.}$ as public broadcast mechanism. The security of the design of the routing protocol starts from this phase a rule is designed to provide dual layer of security for any message being communicated.

This module is created to show that our attacker module is a stronger module to decrypt even this security layer, thereby assist the framework to catch hold of the attacker by determining the infected routes till that instant. This dual layer of security will facilitate data for node j for only estimating $P_{key(i,\ j)}$ with respect to node i without furnishing any information to other node j.

C. Adversarial Model:

Our previous work has already focused on the modelling the behaviour of the attacker node for preventing the decamping mechanism. The uniqueness part of the proposed system is the design of this attacker module where we are considering that this module is extremely strong enough to decrypt any of the information transacted between any authorized mobile nodes by invoking any types of routing attack. The main intention of this module is to intrude or initiate any of the routing attack along with infection spread from dispatcher node D to destined node d with minimum cost of attack. But this time the attacked module is enhance with additional capability by which they can attach an unit cost in resource expenditure needed to initiate an attack. As in wireless sensor network, normally there is no digital certificate authentication among the nodes so, we also consider that this module will attempt to give rise to all issues like route disruption, node isolation, and resource consumption in the defined scenario of the wireless sensor network and they perform all this by extracting the secure keys from the authorized nodes. The model also assumed to posses all the route information G_{Dd} using our previous model.

The proposed system uses the greedy heuristic approach for identifying the probability of attack on WSN. Below given is the proposed algorithm used to detect the attack and it's vulnerability.

Algorithm: To Identify the node capture as well as routing attack in a given WSN scenario

Input: Weight& cost of capturing node& link to next hop node.

Output: Node and route infected.
Steps:

```
1  Given : mobile node parameters
2  Initialize : maximum hop distance
3 Calculate: neighborhood area.
  $Size_{(neigh)} = \{(No.\ of\ Nodes) .(\pi).(Radio\ Range)^2\}/ Deployment\text{-}Area$
4  Design network module
5  Design Cryptographic module
6  Design adversarial module
7  Switch Case (Route Susceptibility):
8 s$S_{key(i, j)} \neq 0$
9 $S_{Dd}(\phi) = 0$
10 $S_{Dd}(A_{nodes}) = 1$
11$0 < S_{Dd}(A_{nodes}) < 1$
12  Estimate current values of all parameters.
13  Based on value of estimated cost calculate the value of
    overall infected link and route cost
14  End
```

The proposed model will estimate the impact of routing attack on the designed security routing protocol considering specified cumulative route CR_{Dd} with the initiation of attack on group of nodes $A_{nodes} \subseteq N$. Let us consider $S_{key(comp)}$ as group of keys being corrupted by the attacker module, which will mean that any packets transmitted through CR_{Dd} which was already encrypted with $S_{key(i)}$ or $S_{key(j)}$ will definitely get compromised by the malicious nodes present within that route. The considered route (i, j) or (D, d) ϵ P_{key} is attacked if and only if $S_{key(i, j)} \subseteq S_{key(comp).}$ and let $P_{key(comp)}$ represents all the attacked routes. Therefore the design of attack on complete route from dispatcher node D to destined node d will represent that any message being communicated using the specified route will definitely get corrupted by the A_{node}. Not only this, the design of the proposed routing protocol also considers the route susceptibility for routing attack when it comes under any of the following criteria:

- $S_{Dd}(\phi) = 0$, which means there is no attack if there is no routes from Dispatcher node D to destined node d.
- $S_{Dd}(A_{nodes}) = 1$, which means that CR_{Dd} is only attacked when there is presence of atleast 1 A_{nodes}.
- $0 < S_{Dd}(A_{nodes}) < 1$, which means the maximum and minimum intensity of attack considering complete route is not attacked but only a portion of it is infected due to routing attack.

IV. Conclusion

In this paper, we presented a mathematical model for node capture attacks in wireless sensor networks. By characterizing the cost of capturing each node and the contribution of each node to the attack success, The proposed paper has examined the issues in designing new efficient and secure routing protocol considering all the routing attack susceptibility parameter in order to enhance the efficiency of the proposed protocol using AODV. A mathematical model is design with algorithm for estimating the impact of majority of the routing attack on wireless sensor network using probabilistic approach using greedy heuristic algorithm. The system finds the successive impact of node and then the route infection. Majority of the implementation done by enhancing cryptographic approach is considered to increase the network overhead which results in poor performance in the network.

REFERENCES

[1] http://www.ietf.org/dyn/wg/charter/manet-charter. Accessed on 6th Dec, 2011

[2] S. Buchegger and J. Boudec, “A robust reputation system for P2P and mobile ad-hoc networks,” in Proc. 2nd Workshop Econ. Peer-to-Peer Syst., 2004, pp. 403–410.

[3] F. Li and J. Wu, “Mobility reduces uncertainty in MANETs,” in Proc. IEEE INFOCOM, 2007, pp. 1946–1954.

[4] A. Josang, R. Ismail, and C. Boyd, “A survey of trust and reputation systems for online service provision,” Decis. Support Syst., vol. 43, no. 2, pp. 618–644, Mar. 2007.

[5] F. Li, A. Srinivasan, M. Lu, and J. Wu, “Uncertainty mitigation for utility-oriented routing in MANETs,” in Proc. IEEE GLOBECOM, 2007, pp. 427–431.

[6] F. Li and J. Wu, “Hit and run: A Bayesian game between malicious and regular nodes in mobile networks,” in Proc. IEEE SECON, 2008, pp. 432–440.

[7] P. Liu, W. Zang, and M. Yu, “Incentive-based modeling and inference of attacker intent, objectives and strategies,” ACM Trans. Inf. Syst. Secur., vol. 8, no. 1, pp. 78–118, Feb. 2005.

[8] G. Theodorakopoulos and J. Baras, “Malicious users in unstructured networks,” in Proc. IEEE INFOCOM, 2007, pp. 884–891.

[9] Kejun Liu, Jing Deng, Pramod K. Varshney, and Kashyap Balakrishnan, “An Acknowledgment-Based Approach for the Detection of Routing Misbehaviour in MANETs”, IEEE Transactions on mobile computing, Vol. 6, NO. 5, May 2007.

[10] Dhanalakshmi, Dr.M.Rajaram ,” A Reliable and Secure Framework for Detection and Isolation of Malicious Nodes in MANET”, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.10, Oct2008

[11] Zan Kai Chong, Moh Lim Sim, Hong Tat Ewe, and Su Wei Tan ,” Separation of Detection Authorities (SDA) Approach for Misbehavior Detection in Wireless Ad Hoc Network”,PIERS Online, VOL. 4, NO. 8, 2008.

[12] S. Buchegger and J.-Y. Le Boudec, “Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes, Fairness in Dynamic Ad-Hoc Networks,” Proc. MobiHoc, June 2002.

[13] Sanjeev Rana, Manpreet Singh, “Performance Analysis of Malicious Node Aware Routing for MANET using Two-Hop Authentication”, International Journal of Computer Applications (0975 – 8887), Volume 25– No.3, July 2011

[14] Rakesh Kumar, Piush Verma, Yaduvir Singh, “Design and Development of a Secured Routing Scheme for Mobile Adhoc Network”, International Journal of Computer Applications (0975 – 8887) Volume 13– No.2, January 2011

[15] Rajib Das, Bipul Syam Purkayastha, Prodipto Das, “Security Measures for Black Hole Attack in MANET: An Approach”, International Journal of Engineering Science and Technology (IJEST), 2011

[16] S. Kannan, T. Maragatham, S.Karthik, V.P. Arunachalam, “A study of Attacks, Attack Detection, and Prevention Methods in Proactive and Reactive Routing Protocols”, International Business Management, 2011

[17] Aishwarya Sagar, Anand Ukey, Meenu Chawla, “Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET”, IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 1, July 2010

[18] Sowmiya Hariharan, Jothi Precia, Suriyakala.C.D, Prayla Shyry, “A Novel Approach for Detection of Routes with Misbehaving Nodes in Manets”, International J. of Recent Trends in Engineering and Technology, Vol. 3, No. 2, May 2010

[19] Usman Yaseen, Ali Zahir, Faraz Ahsan, and Sajjad Mohsin, “Estimating the Effects of Jammers via Conservation of Flow in Wireless AdHoc Networks”, International Journal for Advances in Computer Science, Volume 1, Issue 1, 2010

[20] Sohail Abbas, Madjid Merabti, and David Llewellyn-Jones, “A Survey of Reputation Based Schemes for MANET”, The 11th Annual Conference on The Convergence of Telecommunications, Networking & Broadcasting (PGNet 2010), Liverpool, UK, 21-22 June 2010

[21] Pradip M. Jawandhiya et. al. / International Journal of Engineering Science and Technology Vol. 2(9), 2010, 4063-4071.

[22] Nishu Garg and R.P.Mahapatra, “MANET Security Issues ,” IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.

[23] B. Kannhavong, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto. A study of a routing attack in OLSR-based mobile ad hoc networks. International Journal of Communication Systems, 20(11):1245–1261, 2007.

[24] B. Kannhavong, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour. A collusion attack against olsr-based mobile ad hoc networks. In GLOBECOM, 2006.

[25] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour. A Survey of routing attacks in mobile ad hoc networks. IEEE Wireless Communications, page 86, 2007.

[26] Y. Hu, A. Perrig, and D. Johnson, “Ariadne: A Secure On-Demand Routing for Ad Hoc Networks,” Proc. of MobiCom 2002, Atlanta, 2002.

[27] Y. Hu, D. Johnson, and A. Perrig. SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks. Ad Hoc Networks, 1(1):175–192, 2003.

[28] Y. Hu, A. Perrig, and D. Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. Wireless Networks, 11(1):21–38, 2005.

[29] C. Tseng, S. Wang, C. Ko, and K. Levitt. Demem: Distributed evidence driven message exchange intrusion detection model for manet. In Recent Advances in Intrusion Detection, pages 249–271. Springer, 2006.

[30] C. Tseng, T. Song, P. Balasubramanyam, C. Ko, and K. Levitt. A Specification-Based Intrusion Detection Model for OLSR. LECTURE NOTES IN COMPUTER SCIENCE, 3858:330, 2006.

[31] M.Wang, L. Lamont, P. Mason, and M. Gorlatova. An effective intrusion detection approach for OLSR MANET protocol. In Secure Network Protocols, 2005.(NPSec). 1st IEEE ICNP Workshop on, pages 55–60, 2005.

[32] T. View. Information theoretic framework of trust modeling and evaluation for ad hoc networks. Selected Areas in Communications, IEEE Journal on, 24(2):305–317, 2006.