International Journal of Computer Sciences
April'2017 Issue
ISSN Number: 4142 3453

Secure Dynamic Source Routing for Controlling Black Hole Attack over Mobile Ad hoc Networks

Rajesh S[1] , K.Venkata Rathnam[2]

[1]M.Tech (CSE),PG Scholar ,Department of Computer Science & Engineering, Rao & Naidu Engineering college, ongole,AP.

[2]Associate Professor ,Department of Computer Science & Engineering, Rao & Naidu Engineering college, ongole,AP.

Abstract Wireless sensor networks are emerging as a promising technology and are increasingly being deployed in security-critical applications. Because of their inherent resource-constrained characteristics, they are vulnerable to wide range of security attacks including routing attacks. A black hole attack is one of the most typical routing attacks that seriously affect data collections. A lot of research has been carried out for secure routing process using different mechanisms. This paper focuses on survey of various schemes to improve the routing protocols against various routing attacks and discusses the state-of-the-art. We also analytically investigate the security and performance of the various trust based scheme

Keywords: Black hole attack, Network lifetime, security, Trust, Wireless Sensor Network

1. INTRODUCTION

Wireless sensor networks (WSN) are distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to base station. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance[1]. Today wireless sensor networks are used in many applications, such as industrial process monitoring and control, machine health monitoring, and so on. In spite of all the advantages and applications of Wireless Sensor Networks, there are even some challenges and issues which have to be dealt with the WSN. The most key challenge is its security. There are various kinds of attacks in WSN like Grey hole attack, Wormhole attack, Sinkhole attack, Selective forwarding attack, Black hole attack, Denial of service attack etc. which will affect the data collection during routing process.

Routing Protocols [12] are generally classified into three types such as Proactive (Table Driven), Reactive (On Demand) and Hybrid based on route discovery process and their mechanism. The Proactive routing protocols select the routes to all destinations at beginning and maintain using periodic update process based on their mechanism. e.g. DSDV. The disadvantages of these algorithms are to update the routing tables often which take a large amount of memory, bandwidth and power. But, in the reactive routing protocol, there is no need to maintain the routing data in routing table by each node. The routes are selected and maintained only when they are required by the source for data transmission during route discovery process and the routing overhead has been reduced. e.g. Dynamic Source Routing (DSR) and Adhoc on Demand Distance Vector (AODV). The merits of both proactive and reactive protocols are combined and form a hybrid routing protocols e.g. ZRP, TORA. The paper is organized as follows. In Routing attacks in the WSN are reviewed. Security and performance analysis are provided in other sections. We conclude in conclusion.

II LITERATURE SURVEY

Y. Liu et al. [6] introduced a truest based secure routing scheme for sensor networks. It supports reliable and scalable communication over network. It uses criteria of residual energy to discover multiple paths. Simulation results show its efficiency in terms of enhancing the probability of security and energy consumption.

H. Moudni et al. [7] enhanced the existing AODV routing protocol for resisting the Black hole attack over MANETs. It monitors the RREQ, RREP and Sequence numbers, if any node receives multiple control messages, it ignores the RREP messages after verification of each forwarding message. Simulation results show its performance in terms of improved PDR and minimum delay under the constraints of mobility in compromised network.

A. O. Alkhamisi et al. [8] introduced trust based secure routing for multiple paths routing over ad hoc networks. It defends against various attacks i.e. Flooding, Black hole and Gray hole attack. It analyzes control messages flow and adds trust value. Finally, Threshold statistics are used to identify the attacks. Simulation results show the its performance in terms of minimum route selection time, control overhead, trust non-utilization factor and energy efficiency etc.

H. Moudni et al. [9] investigated the impact of various attacks over the density of traffic, network size, node mobility under various performance constraints i.e. Delay, PDR and Throughput etc. Simulation results show that in case of Black hole attack, Throughput decrease where as Routing load increases. As compared to other attacks i.e. Rushing, flooding, Black hole attack has the highest impact over network performance.

S.Uma maheswari et al. [10] developed a solution to secure the network from Denial of Service attack. It can filter out the HELLO message flooding over network which can cause data transmission interruption and may result is packet loss at large scale. It offers minimum key exchange time and keeps the track

of each control message exchange.

Emimajuliet.P et al. [11] presented a solution to secure the MANETs by intruders by identifying the transmission range and packet loss ratio over that particular range. Node level statistics are verified to know the most critical path which has the highest packet loss and finally, intruder over that path is discovered. Simulation results show that it can maintain network performance in the presence of malicious nodes.
Pooja et al. [12] presented a solution to detect the Black hole attack using Hint Based Probabilistic routing method under the constraint of various mobility models. Trusted authority is used to build the HINTS for each node which is participating in transmission and its HINT is compared against a predefined Threshold value, if HINT does not satisfy the Threshold value, it is marked as malicious node and hence neglected for routing purpose, finally communication is initiated using reliable and secure paths. Simulation results show that it is able to analyze the packet drop and overhead in the network and proposed solution can be further extended Black hole attack detection and removal.
J. Ponniah et al. [13] developed a protocol suit to guard the ad hoc networks from security threats. It can analyze the multiple layers and defines set of rules for each one and makes an assumption that intruder cannot intercept the data at all layers, in one attempt. It starts network tracing, when any node joins the network. It collects the node level statistics and compares it with the node's history. Statistic evaluation is used to detect the malicious node using consistency check algorithm which regulates the transmission and reception of data. It defines various models i.e. Node Model defines the terms for legitimate and malicious nodes on the basis of their states, Communication Model defines the terms for data transmission and reception and keeps the track of signal jamming also, Clock Model defines the timer for communication purpose, Key based security method assigns keys to each node which are use for secure communication, Utility function defines the Throughput rate and link rate vectors and if nay ode nodes which cannot fulfill this criteria, is not eligible for communication. Analytical analysis shows that combination of multiple features can provide the robust security for ad hoc networks. B.Ballav et al. [14] developed a zone based routing solution to encounter the black hole attack over mobile sensor networks. It keeps the track of packet flow between base station and intermediate odes and uses acknowledgement for each packet. If node does not send ACK control packet and drops all packets, then it is identify as intruder. Simulation shows that it consumes less energy for monitoring purpose and is able to maintain the network performance under QoS constraints.

III. PROPOSED WORK

Proposed scheme stars traffic monitoring, only if it is essential to diagnose the network. On the basis of reasoning, decision is made to avoid that route. After blocking the route, network operates in normal environment till the detection of next node misbehavior. If there is any black hole attack, first of all intruder will alter the routing information and then acquiring the route, it will start packet drop, so all activities will be executed at same time, So we sub divide the packet drop into three different categories: Normal Packet , Packet Forwarding Drop and Unknown Packet Drop. In normal packet drop condition, packet drop may occur due to buffer over flow or due to route error but if it starts at the time when a packet is forwarded to next hop and intermediate node just drop it and after that it drops all the packets simultaneously. Thus result in the all types of packet drops i.e. Normal, forwarding and Unknown and its source can be detected using various routing attributes such as Current node index, current route length and NEXT Hop etc. Proposed scheme will trace the routes, if requested otherwise it will remain silent.

```
If (Black Hole Attack==1)
 {
If (routing))
{Rl Rl: Get Route->Length ()
I: Get Route->Index ()
N: Set Route->PKT->Drop Count (Rl, I, Normal)
F: Set Route->PKT->Drop Count (Rl, I, Forwarding)
U: Set Route->PKT->Drop Count (Rl, I, UNKNOWN)
If (N=1 && F==true && U ==true)
{For each Rl && I TH++;
Start (Trace Route (Rl, I, Node->Index);)
UpdateRouteTh (Rl, I, Node->Index);
 Reasoning: If (Th> x)
{ ignore Route (Rl, I, Node->Index); exit (Trace Route ()) } } } }
```

IV METHODOLOGY

There are different kinds of attacks [3], [8], [11] possible by malicious nodes to harm the network and make the network unreliable for communication and proper functioning. Some of such kinds of attacks are: Wormhole Attack: Wormhole attack is an attack on which the messages are Tunneling and replicating from one location to another through alternative low latency links, that connect two or more points (nodes) of the WSN by using more powerful communication resources than normal nodes and establishing better real communication channels (called tunnel). Wormhole nodes operate fully invisible. Sinkhole Attack: Sinkhole attack Attract or draw the all possible network traffic to a compromised node by placing a malicious node closer to the base station and enabling selective forwarding

Selective Forwarding Attack: In a selective forwarding attack, a compromised node refuses to forward some of the packets in its outstanding buffer, such as control information or data packets in order to cut off the packets propagation. Black hole Attack: A black hole is a attack in which malicious node attracts all the traffic in the network by advertising that it has the shortest path in the network. So, it creates a symbolic black hole with the malicious node or the adversary at the center. This black hole drops all the packets it receives from the other nodes. Grey hole Attack: A Grey hole is similar to the black hole attack except that the malicious node selectively or randomly forwards/drops only some of data packets that they are routed through it, at random intervals to protect from its forged/artificial path. Also a kind of Denial of Service attack that the attacker receives but does not forward all incoming messages. Denial of Service Attack: A

Denial of Service (DoS) attack is one that attempts to prevent the victim from being able to use all or part of his/her network connection. DoS attack allows an adversary to subvert, disrupt, or destroy a network, and also to diminish a network's capability to provide a service

In this paper, we have analyzed a various novel security and trust based routing scheme against black hole attack and presented their performance over the packet delivery ratio. From the above analysis, we can conclude that ActiveTrust scheme is the efficient scheme for detecting and preventing the black hole attack among other schemes. The ActiveTrust scheme has the following excellent properties: (1) High successful routing probability, security and scalability. The ActiveTrust scheme can quickly detect the nodal trust and then avoid suspicious nodes to quickly achieve a nearly 100% successful routing probability. (2) High energy efficiency. The ActiveTrust scheme fully uses residue energy to construct multiple detection routes. The theoretical analysis and experimental results have shown that this scheme improves the successful routing probability by more than 3 times, up to 10 times in some cases. Further, ActiveTrust scheme improves both the energy efficiency and the network security performance. It provides important significance for wireless sensor network security.

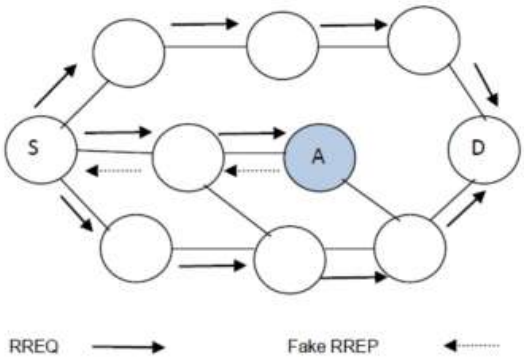

Figure 1. Example of a Black Hole Attack on DSR.

TARF: A Trust-Aware Routing Framework: For a TARF [4] enabled node N to route a data packet to the base station, N only needs to decide to which neighboring node it should forward the data packet considering both the reliability and the energy efficiency. Once the data packet has been forwarded to the next-hop node, the remaining task to deliver the data to the base station is fully delegated to it, and N is totally unaware of what routing decisions are made by its next-hop node. The node N maintains a neighborhood table with trust level values and energy cost values for certain known neighbors. EnergyWatcher is accountable for recording the energy cost for each known neighbor, based on N's surveillance of one hop transmission to reach its neighbors and the energy cost report from those neighbors. TrustManager is responsible for tracking the neighbors trust level values based on network loop discovery process and broadcast messages from the base station about data delivery. Once N is able to choose its next-hop neighbor according to its neighborhood table, it sends out its energy report message. Its energy cost is broadcasted to all its neighbors to deliver a packet from the node to the base station.

Hierarchical Trust Management: Hierarchical trust management protocol [5] maintains two levels of trust: SN-level trust and CH-level trust. Each Sensor Node (SN) evaluates other SNs in the same cluster while each Cluster Head (CH) evaluates other CHs and SNs in its cluster. The peerto-peer trust evaluation is updated periodically based on either direct observations or indirect observations. When two nodes are within radio range, they evaluate each other based on direct observations via snooping or overhearing. Each SN sends its trust evaluation results toward other SNs in the same cluster to its CH. Each CH performs trust evaluation for all its SNs within its cluster. Similarly, each CH sends its trust evaluation results through other CHs in the WSN to a "CH commander" which may reside on the base station , or on a CH elected if a base station is not available. The CH commander performs trust evaluation toward all CHs in the system. Hierarchical trust management protocol can be applied to two applications namely Trust-based geographic routing and Trust-based intrusion detection application

Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol: In this work [7] the focus is on providing the security in routing protocol with concern to privacy, authentication and nonrepudiation of the data in the network. The security in Energy Efficiency Node Disjoint Multipath Routing Protocol (EENDMRP) [6] is analyzed using RSA Public key crypto system. During the route construction phase, the sink node broadcasts Route Construction (RCON) packets to its neighbouring nodes. The neighbouring nodes receive the RCON packet from the sink node. A neighbouring node updates RCON packet with its public key. It rebroadcast the RCON packet to its neighbouring nodes. Similarly all the nodes update their routing table with the public key of their neighbouring nodes in the network. In the data transmission phase, the source node will select node-disjoint paths to the sink node and sends the data traffic through that path. The source node picks M amount of data to send through the node-disjoint primary path to the sink. The MD5 hash function H is used to create message digest H(M) from the M amount of data at the source node. The source node generates the digital signature by encrypting the message digest H(M) with its private key. The source node forwards it to neighbouring node through the path it takes to reach sink. A neighbouring node verifies the digital signature by comparing decrypted value. If the generated H(M) by the receiver and the decrypted H(M) of digital signature is equal, then the receiver accepts the data. Otherwise rejects the data and informs the sender that the data is altered through by generating route error packet.

IV. CONCLUSION

MANETs are wireless based networks of mobile nodes with limited resources like computation power, communication range and storage capabilities, shared channel, usually for economical reasons. There is no centralized authority to monitor the nodes and nodes can join and leave the network any time. So if any malicious node joins the network then it is very difficult to trace that node. So it is necessary to detect

and isolate that node from entire network for smooth operations. To secure the communication over MANETs there must be a method which can ensure the detection and prevention from the attacks like Black Hole. Mobile ad hoc network resources suffer from this attack. This research work analyzes the impact of black hole attack over MANET and proposed a method which is able to handle black hole attack over DSR.

REFERENCE

1. Ashutosh Bhardwaj, "Secure Routing in DSR to Mitigate Black Hole Attack", ICCICCT-IEEE-2014, pp.985-989.

2. Prachee N. Patil, Ashish T. Bhole, "Black Hole Attack Prevention in Mobile Ad Hoc Networks using Route Caching", IEEE-2013, pp.1-6.

3. Mahmood Salehi, Hamed Samavati, "DSR vs. OLSR: Simulation based Comparison of Ad hoc Reactive and Proactive Algorithms under the Effect of New Routing Attacks", International Conference on Next Generation Mobile Applications, Services and Technologies, IEEE-2012, pp.100-105.

4. D. A. Malt z, J. Broch, J. Jet cheva, and D. B. Johnson, "The effects of on-demand behavior in routing protocols for multi-hop wireless adhoc networks," in IEEE Journal on Selected Areas in Communications special issue on mobile and wireless networks, August 1999.

5. Houda Moudni, Mohamed Er-rouidi, Hicham Mouncif, Benachir El Hadadi, "Attacks against AODV Routing Protocol in Mobile Ad-Hoc Networks", International Conference Computer Graphics, Imaging and Visualization, IEEE-2016, pp.385-389.

6. Y. Liu, Mianxiong Dong, Kaoru Ota, "ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks", IEEE Transactions on Information Forensics and Security, IEEE-2016, Vol.11 (9), pp.2013 – 2027.

7. H. Moudni, Mohamed Er-rouidi, Hicham Mouncif, Benachir El Hadadi, "Modified AODV Routing Protocol to Improve Security and Performance against Black Hole Attack", IT4OD, IEEE-2016, pp.1-4.

8. A. O.Alkhamisi, Seyed M Buhari, "Trusted Secure Adhoc On-Demand Multipath Distance Vector Routing in MANET", International Conference on Advanced Information Networking and Applications, IEEE-2016, pp.212-219.

9. H. Moudni, Mohamed Er-rouidi, Hicham Mouncif, Benachir El Hadadi, "Performance Analysis of AODV Routing Protocol in MANET under the Influence of Routing Attacks", ICEIT, IEEE-2016, pp.536 – 542.

10. S.Uma maheswari, N.S.Usha, E.A.Mary Anita, K.Ramaya Devi, "A Novel Robust Routing Protocol RAEED to Avoid DoS Attacks in WSN", ICICESIEEE-2016, pp.1-5.

11. Emimajuliet.P, Thirilogasundari.V, "Defending Collaborative Attacks in Manets Using Modified Cooperative Bait Detection Scheme", ICICES, IEEE- 2016, pp.1-6.

12. Pooja, R. K. Chauhan, "AN ASSESSMENT BASED APPROACH TO DETECT BLACK HOLE ATTACK IN MANET", ICCCA, IEEE-2015, pp.552 – 557.

13. J. Ponniah, Yih-Chun Hu, P. R. Kumar, A System-Theoretic Clean Slate Approach to Provably Secure Ad Hoc Wireless Networking, TCNS-IEEE-2016, pp.206 – 217.

14. Bikram Ballav, Gayatree Rana, Dr. Binod Kumar Pattanayak, "Investigating the effect of Black Hole attack on Zone Based Energy Efficient Routing Protocol for Mobile Sensor Networks", ICIT, IEEE-2015, pp.113-118.

15. Yuxin Liu, Mianxiong Dong,Kaoru Ota, and Anfeng Liu, "ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks", IEEE Transactions On Information Forensics And Security, Vol. 11, No. 9, PP. 2013 – 2027, September 2016.

16. Tao Shu, Marwan Krunz, and Sisi Liu, "Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes ," IEEE Transactions on Mobile Computing, Vol.9,No.7,PP.941-954,July 2010.

17. Ming-Yang Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems" ,Elsevier-Computer Communication,Vo;.34, pp-107-117, August 2010.

18. Guoxing Zhan, Weisong Shi and Julia Deng, "Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs", IEEE Transactions On Dependable And Secure Computing, Vol. 9, No. 2, PP.184-197, April 2012.

19. Fenye Bao, Ing-Ray Chen, MoonJeong Chang, and Jin-Hee Cho, "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection" , IEEE Transactions On Network And Service Management,Vol.9, No. 2, PP.169-183, June 2012.

20. Anfeng Liu, Zhongming Zheng, Chao Zhang, Zhigang Chen and Xuemin (Sherman) Shen, "Secure and Energy-Efficient Disjoint Multipath Routing for WSNs," IEEE Transactions On Vehicular Technology, Vol. 61, No. 7, PP. 3255-3265, September 2012.

21. Shiva Murthy G, Robert John D'Souza, and Golla Varaprasad, "Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks", IEEE Sensors Journal, Vol. 12, No. 10, PP.2941 -2949, October 2012.

22. M. Mohanapriya ⇑, Ilango Krishnamurthi, "Modified DSR protocol for detection and removal of selective black hole attack in MANET," ELSEVIER Computers and Electrical Engineering,Vol.40, PP.530–538, June 2013.

23. Abderrahmane Baadache , Ali Belmehdi, " Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks," ELSEVIER Computer Networks, Vol.73, PP. 173–184, August 2014.

24. Adnan Ahmed, Kamalrulnizam Abu Bakar, Muhammad Ibrahim Channa, Khalid Haseeb, and Abdul Waheed Khan, "TERP: A Trust and Energy Aware Routing Protocol for Wireless Sensor Network," IEEE Sensors Journal, Vol. 15, No. 12, PP. 6962-6972, December 2015.

25. Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-

Chieh Chao, and Chin-Feng Lai, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach," IEEE Systems Journal, Vol. 9, No. 1,PP.65-75, March 2015.

26. Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao," A survey of black hole attacks in wireless mobile ad hoc networks" , Springer-Human-centric Computing and Information Sciences, 2011, 1:4.