Securing Mint Route Protocol in Wireless Sensor Networks

Lakshmi S. Gopal, Arjun S., Remya Nair T.

ABSTRACT---The proposed research work is an attempt to build an algorithm to resolve an intrusion attack namely; the sinkhole attack from MintRoute protocol, being one of the most commonly used routing protocols in wireless sensor networks. This paper illustrates the working of the protocol and studies it in detail. We emphasize on strategies that an attacker can choose to launch a sinkhole attack. Then we attempt to propose a specific algorithm that may reduce the intrusion threats in wireless sensor networks.

KEYWORDS: Wireless Sensor Networks (WSN), Sinkhole Attack, MintRouteProtocol,LightweightExtensibleAuthentication Protocol (LEAP)

I. INTRODUCTION

Wireless Sensor Networks (WSN) is one of the most demanding and emerging technologies that supports innumerable applications that are extensively used in various fields such as military applications, environmental sensing, education, health care, inventory control and so on. WSN consists of a number of sensor nodes which are vastly distributed in the environment to track various physical conditions such as sound, weight, temperature etc. WSN mainly senses data and the data analyzed is passed to a computation centre called base station which computes the collected data.

Generally, the nodes of a WSN has several parts namely, a radio transceiver (a device that comprises of both transmitter and a receiver), internal antenna, a microcontroller (a small computer on a single integrated circuit) and an electronic circuit for interfacing with sensors. There are several network topologies on which WSNs can be implemented, varying from a simple star network to an advanced multihop wireless mesh network. Routing is a common technique which propagates signals between the hops in a network.

The nodes in a WSN is basically a low cost, low memory device and operates mostly in public or in-house environments and hence they are vulnerable to several security issues. WSNs are exposed to various intrusion attacks such as denial of service, sybil attack, wormhole attack, flood attack, sinkhole attack etc. Among these, WSNs are most commonly susceptible to sinkhole attack.

A. Sinkhole Attack

Sinkhole attack is one of the most vulnerable attack in the network layer of a WSN. The network layer is in charge of escorting the information that is passed on from the transport layer. The network layer is susceptible to various attacks andan intruder can easily exploit it since the routing protocols are unaware of these attacks. Generally, in a sinkhole attack an intruder chooses a node to attack the network and this node is called as a compromised node. The compromised node attracts the entire network to itself so that all the data passes through it and the intruder gets access to it. The intruder chooses either the node that is closer to the base station or a node that is located in a populous area of the network. The compromised node adopts many mechanisms to attract the network like announcing a low hop count to the base station or by declaring an exceptional connection to the base station. Once the compromised node attracts the network towards itself, it gets access to the data and can perform catastrophic operations like altering the data, data loss, forward the data to other intruders and so on. There are several routing protocols that are vulnerable to sinkhole attack such as MintRoute protocol, Multihop LQI protocol, AODV protocol etc. From this study we understand the weakness of these protocols and the relevance of enhancing them by incorporating countermeasures. This paper focuses on how to secure MintRoute protocol from sinkhole attack.

B. MintRoute Protocol

It is a new standard routing protocol that has a layered approach and it is basically designed for TinyOS. TinyOS is an embedded, component based operating system and it is a platform for low power devices like a sensor in a WSN. It uses NesC programming language which is a dialect of C language and is optimized for the memory limits and power consumption limits of these devices. In this protocol routing decisions are mainly based on the link quality estimates rather than minimum hop count and chooses the best route to send data from a source node to the base station.

The nodes in a WSN often obstruct high reliability and all the previously mentioned applications demands for it. Even though MintRoute protocol chooses the best route to traverse, there are chances that an intruder can attack and trace the route and get access to the network. MintRoute protocol is one among those protocols that are susceptible to sinkhole attack. An intruder can intervene into the best route chosen by the protocol and make one of the nodes as the compromised node to launch more attacks.

This paper focuses on enhancing MintRoute protocol by securing it from sinkhole attack. There are several traditional security mechanisms like authentication,

Revised Manuscript Received on May 29, 2019.

Lakshmi S. Gopal, PG Student, Computer Application, Amrita VishwaVidyapeetham School of Arts and Sciences, kochi, Kerala, India

Arjun S., PG Student, Computer Application, Amrita VishwaVidyapeetham School of Arts and Sciences, kochi, Kerala, India

Remya Nair T, Assistant Professor, Computer Application, Amrita VishwaVidyapeetham School of Arts and Sciences, kochi, Kerala, India

symmetric key encryption & decryption etc, which can be used to administera secure transmission of data between these nodes. But the real challenge is to implement these security mechanisms onto the routing protocols of a wireless network.

II. LITERATURE REVIEW

To many, WSNs are exceedingly challenging and has an integral scope in research works. Secure transmission of data between nodes of a wireless network is a backbreaking task. We noticed that there are several attacks that crop up in various protocols that are used for communication between nodes in a wireless network. We studied a survey on WSNs and their security issues[3] and it suggested few generic solutions to it. Although, there are numerous countermeasures introduced by many, but there are fewer solutions for intrusion attacks in WSNs.

We scrutinized various research works that illustrated some existing routing protocols that are vulnerable to several attacks in WSNs[1][4][15][16][17][21][22]. As reported by their studies, sinkhole attack is one of the most defenseless attacks in WSNs[1][18]. We analysed all the routing protocols that are susceptible to sinkhole attack and how a sinkhole attack can be activated on these protocols[22].

One of the major setback found in these protocols is how data can be transmitted over the network reliably. MintRoute Protocol is a well-known approach used in WSNs for routing purposes. MintRoute Protocol is a new metric that considers the link quality for path selection in WSNs. We reviewed several existing works on this domain and found an algorithm for MintRoute Protocol that calculates the link quality of the links between the nodes and the one with greater quality is chosen for transmission of data[4]. It considers several parameters to calculate the link quality and the algorithm emerged successful in transmitting data reliably and reduces end to end delay as well. This paper focuses on enhancing this protocol by providing information security while data is transmitted between nodes in a wireless network.

Generally, information security is the state of being protected against the unauthorized use of information. There are numerous approaches used to provide information security is wireless networks. Key distribution is a common mechanism used for secure transmission of data. This paper attempts to proposes an algorithm that incorporates LEAP protocol[5], a key distribution technique that strengthens the existing algorithm of MintRoute protocol. By implementing this technique we try to reduce the chances of Sinkhole attack in MintRoute protocol.

III. ANALYSING SINKHOLE ATTACK IN MINTROUTE PROTOCOL

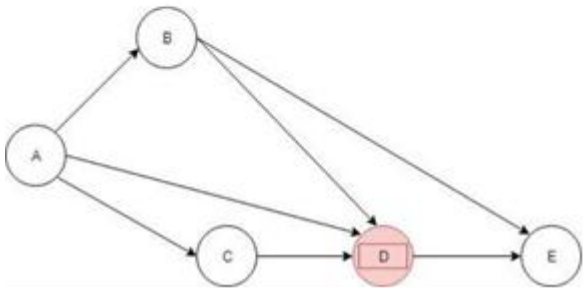
In MintRoute protocol packet is sent by choosing the best route in the network rather than considering the minimum hopcount between the nodes. Generally, link quality estimates is calculated by packet error rate. It is the number of error packets after Forward Error Correction (FEC - technique used for controlling errors in data transmission over noisy channels). Every node broadcasts a packet regularly called as the route update packet which contains the link quality estimates and each node evaluates the link quality of its corresponding neighbours using the route update packet. Every node maintains a neighbour table which contains the identification of its neighbours and corresponding link qualities and this table is updated periodically using the route update packet.

The source node selects a neighbour node according to the estimates from the neighbour table to carry out data transmission. The selected node is called as the parent node. Suppose more than one neighbour node has the same link quality then minimum hop count is considered for parent selection. Suppose any node in the network gets 75% greater link quality than the present parent node or the present parent drops below 25% then a parent changing mechanism is activated. This process is vulnerable to various attacks and sinkhole attack is a predominant one.

Neighbour table of A

Node	Quality
B	120
C	225
D	80

Before attack

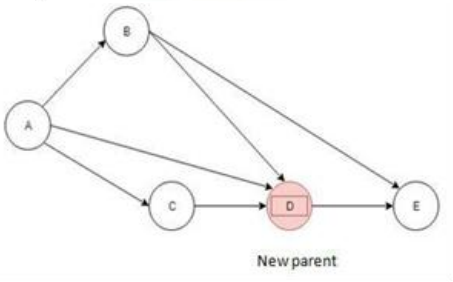


Consider the above network with 5 nodes and node A is the source node and node E is the destination. Nodes B,C and D are the neighbour nodes of A. The above table represents the route update packet received by A and it shows that node C has the highest link quality and A chooses C as the parent node. Suppose an attacker attacks on node D and it wants to attract the source node by malicious means. So the attacker attracts node A by updating the route update packet of node D and upgrades its value and is sent to node A. Just by improving the link quality of the compromised node will not activate the parent changing mechanism. If the current parent has a considerable link quality then it need not change the parent node. So the attacker diminishes the link quality of the present parent and upgrades the compromised node.

Neighbour table of node A

Node	Quality
B	120
C	20
D	225

After attack



The above table represents the neighbour table of node A updated using the route update packet received from the compromised node. The attacker has now increased the link quality of the compromised node and the source node activates parent changing algorithm and selects node D as the new parent. Now the attacker has access to the network and since it is closer to the destination node E, all the data will pass through the compromised node and the attacker has access to it. This is how sinkhole attack arises in MintRoute protocol. This paper focuses on how security can be provided in data transmission in MintRoute protocol and prevent the occurence of sinkhole attack.

IV. PROPOSED SYSTEM

Providing security in MintRoute protocol can be accomplished by revising the parent changing algorithm since it is the most vulnerable section of the protocol. This paper attempts to propose an algorithm that ensures reliable data transmission and reduces end to end delay between nodes of a network. The following algorithm secures the MintRoute protocol using LEAP(Lightweight Extensible Authentication Protocol) mechanism.

A. Algorithm

1). Key Pre distribution phase :

Con ⟶ i :$K_{Initial}$ || $K_{Initial}$: $K_i = f_{Initial}(i)$

2). Select best neighbouring node (n) on the basis of (1) and is designated as B(t).

3). For a node n

If(Link i , nn(t) (t)= =0)

Bi(t) = n

Else

If(Linki ,nn(t) (t) x Delay_factor) > (Link i,n(t) (t) x Link n, nn(t) (t))

Bi(t) = Bnn(t) (t)

4). Neighbourdiscovery :

a). i ⟶ * : i

b). j ⟶ i :j,MAC(Kj,i,j)

5). Pairwise key :

a). i ⟶ j : Ki,j = f Kj

b). j ⟶ i :Kj,i= f Ki

6). Key erasure :

a). Delete KInitial from i.

The above algorithm incorporates two protocols namely, MintRoute protocol and LEAP. LEAP is a deterministic scheme that provides a mechanism to establish a pairwise key between two neighbouringnodes[5]. The initial step is a key predistribution phase which generates an initial key by the controller and is denoted by Kinitial for every node in the network. Kinitial is accessed by the nodes using its master key K. The best neighbour node ‘n’ is selected based on the following equation and it is designated as B(t)

$$Link_{i,j}(t) = Q_{i,j}(t) \times P\_DR_{i,j}(t) \quad (1)$$

whereLinki,j(t) represents the link quality between source node i and destination node j. Qi,j(t) is a quality factor that is determined using two indicators namely, RCPI(Received Channel Power Indicator) and PSNI(Perceived signal to noise indicator). The former analyses the signal power and returns the value,

$$RCPI = Signal + Noise + Interference \quad (2)$$

The latter analyses the signal post processing and returns a value that is signal to noise plus interference. So to calculate the value of Q,

$$Q = RCPI\ value - PSNI\ value \quad (3)$$

The next factor included in (1) is the packet delivery ratio which is calculated using the following equation,

$D\_PR_{i,j}(t)$ = N successful packets / N successful packets + N missed packets(4)

By integrating the above two quality factors signal strength between two nodes can be found out and the node with the best link quality will be selected as the parent node. The best neighbour node is denoted as B(t).

Once the best neighbour node is selected data transmission can take place. But to reduce end to end delay an extra procedure is included where the source node checks the link quality of the neighbour node of its parent node which can be called as the grandparent node. In this algorithm it checks if the grandparent node(denoted as nn(t)) is in the transmissionrange of the source or not. If Link i,nn(t) (t) equals to zero then it means that the grandparent node is out of the source’stransmission range and the current parent node can be chosen. If it is not equal to zero then the algorithm goes to its else part. Here it first checks for the link quality between the source and the grandparent node and is multiplied to a delay factor since the grandparent node could be geographically far from the source. This result i compared with the link qualities of source-parent and parent-grandparent nodes. If the grandparent node has the greater value then it can be chosen to perform the data transmission.

Now the source has found its best neighbour node.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

According to the concepts of LEAP, it generates a pairwise key distribution between the two nodes. So the next process is neighbour discovery phase where the source sends a message to the destination along with its identification to inform that a data transfer is on the way. Once the destination receives this message it replies a message that includes its identification, master key and the source identification using a MAC(Message authentication code). By doing so a connection is established between the nodes.

Once this phase is done, it can go further by establishing a pairwise key between them. The source sends a pairwise key to the destination and the destination can access it using the master key and vise versa. Now both the nodes have a session key so that data can be transmitted safely.

Once the data is sent the source node can perform the last step that is, the key erasure phase where the initial key of source is erased. By incorporating LEAP mechanism in MintRoute protocol sinkhole attack can be prevented.

V. CONCLUSION

We have concluded from our studies that sinkhole attack is one of the most vulnerable intrusion technique in WSNs. This paper attempts to illustrate an algorithm that incorporates LEAP mechanism into the MintRoute protocol. In this paper we determine the link quality using two factors, delivery ratio and Q factor rather than the minimum hop count to choose the best neighbour node. These quality factors does not increase payload of sensor nodes since it just requires circuits for its functioning. LEAP is a deterministic key distribution method and hence the network is secured from any intrusion in an assumed time period. Key distributions can be performed by the controllers in each node. The efficiency of this algorithm faces a challenge if the network resides in a dense area or has innumerous nodes. Thus related to work, power consumption remains as a main research challenge.

REFERENCES

1. Generation Mechanisms Of Sinkhole Attack in Routing Protocols of Wireless Sensor Network- Amitkumarjangid, Dr. Nonitasharma, Ankurbohora
2. System and method for Received Channel Power Indicator(RCPI) measurement- Joseph A Kwak, Stephen G Dick
3. A Survey on Wireless Sensor Networks Security- AbhishekPandey, R.C. Tripathi
4. Evaluating revised MintRoute protocol in wireless sensor networks - Ki-Il Kim and Tae-Eung Sung
5. Information Security in Wireless Sensor Networks - AbdelraoufOuadjaout, MiloudBagaa, AbdelmalikBachir, YacineChallal,NouredineLasla, LyesKhelladi
6. An effective handling of secure data stream in IoTJaejinJanga, Im.YJunga, Jong HyukParkes
7. SecureSense: End-to-end secure communication architecture for the cloud-connected Internet of Things ShahidRaza a,, TómasHelgason a, PanosPapadimitratos , Thiemo Voigt
8. SIoT: Securing Internet of Things through distributed systems analysis , Fernando A. Teixeira, Fernando M.Q. Pereira, Hao-Chi Wong, José M.S. Nogueira, Leonardo B. Oliveira
9. Internet of things: Privacy issues revisited Rolf H. Weber
10. Secure routing for internet of things: A survey David Airehrour, Jairo Gutierrez , Sayan Kumar Ray
11. A survey of intrusion detection in Internet of Things, Bruno BogazZarpelãoa, Rodrigo SanchesMianib, Cláudio Toshio Kawakania, Sean Carlisto de Alvarengaa
12. An access control management protocol for Internet of Things devices Mark Taylor, Denis Reilly and Brett Lempereur, Liverpool John Moores University
13. Energy-efficient mechanisms in security of the internet of things: A survey, HamedHellaoui a, MouloudKoudil a, AbdelmadjidBouabdallah
14. A Survey on Detection of Sinkhole Attack in Wireless Sensor Network George W. Kibirige, CamiliusSanga
15. Sinkhole attack detection based on redundancy mechanism in wireless sensor networks Fang-Jiao Zhanga, Li-Dong Zhaia , Jin-Cui Yangb, Xiang Cuic
16. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, Chris Karlof David Wagner
17. Security Analysis of Routing Protocols for Wireless Sensor Networks - Celia John, CharuWahi
18. Launching a Sinkhole Attack in Wireless Sensor Networks; the Intruder Side - IoannisKrontiris, ThanassisGiannetsos, TassosDimitriou
19. Wireless Sensor Network Security: A Survey - John Paul Walters, Zhengqiang Liang, Weisong Shi, and VipinChaudhary
20. Wireless sensor network survey - Jennifer Yick, Biswanath Mukherjee, DipakGhosal
21. A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures - FurrakhShahzad, Maruf Pasha, Arslan Ahmad
22. Sinkhole Attack Detection and Prevention in WSN & Improving the Performance of AODV Protocol- NeelamJanakkumar Patel, Dr. KhushbooTripathi

AUTHORS PROFILE

Lakshmi S Gopal, PG Student, Master of Computer Application, Amrita VishwaVidyapeetham School of ArtsandSciences,Brahmasthanam,EdappallyNorth P.O. Kochi - 682 024, Kerala.

Arjun S, PG Student, Master of Computer Application, Amrita Vishwa, Vidyapeetham School of Arts andSciences, Brahmasthanam, Edappally North P.O. Kochi - 682 024, Kerala.

Remya Nair T, Assistant Professor, Dept. of CS & IT, Amrita School of Arts and Sciences, Kochi, Amrita ViswaVidyapeetham. Qualification: Master of Computer applications, CCNA. Paper Publications:Improving TCP performance in MANET using signal strengthening and scalable TCP - Volume 10, Issue 55, 2015, Pages 728-1731, ISSN: 09734562SourceType: Journal Original language: EnglishDocumentType:ArticlePublisher: Research India Publications