DETECTING BLACK HOLE ATTACK AND SECURE MULTIPATH ROUTING PROTOCOL IN WIRELESS SENSOR NETWORKS

Balaraju G

ABSTRACT: Wireless Sensor Networks (WSN) suffers from variety of threats such as operational lifetime of sensor nodes and security for information carried by sensor nodes. There is an increasing threat of malicious nodes attack on WSN. Black Hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in network. Here we propose an approach to secure the multipath routing protocol in WSN by authentication process. The multipath routing protocol ensures the long life span of the wireless sensor network.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) made up of spatially scattered free little arranges (gadgets) that understandingly check biological (natural) or goal (physical) circumstances in inaccessible (remote) and every now and again unfavourable situations. WSNs as an uncommon instance of Mobile Ad-Hoc Networks (MANETs) are firstly roused by military applications, for example, fringe observation and combat zone checking. Today's WSNs can be utilized as a part of different non military personnel applications, for example, home computerization, activity control, health awareness and natural surroundings checking. Wireless Sensor Networks comprises of numerous particular qualities (includes) that detail them perceivable (recognizable) from traditional (conventional) sensor networks. At first, WSNs ordinarily work in unattended ranges and additionally contain an enormous number of sensor hubs, which can be in the direct of thousands hubs. These hubs contain

extremely inadequate assets as far as vitality, memory, correspondence and computational force. Because of such asset restrictions, consistency and exactness of a solitary remote sensor hub is altogether accordingly require community information gathering and preparing. Likewise on account of the basic and inconsistent. Hardware, sensor nodes may end sooner than their normal lifetime. Consequently, the quantity of sensor nodes may likewise get changed in the system lifetime in an enthusiastic (element) evolving topology. To utilize WSNs in real (genuine) world applications, these particular elements of WSN must be precisely tended to amid the convention plan. Security is another unmistakable component of WSNs and it is an essential tension (worry) so as to give bound (secured) and validated correspondence among sensor nodes in mission basic applications, similar to military or social insurance association. As in whatever other remote system (case subjective radio systems or radio recurrence ID systems), essential security administrations of WSNs incorporates verification, Secrecy, privacy, uprightness, obscurity and accessibility.

II. LITERATURE SURVEY

2.1 Security Protocols:

Security protocols such as AOMDV protocol, Energy Efficient protocol, LIEMRO protocols, PNDMSR protocol, and SEEM protocol are used to route the packet or information from source to destination or source to the sink since the existing protocols are not efficient to transfer a data to destination or sink because the network overhead is high. Since the performance of the protocols is very low. To surveyed all the existing protocols the best efficient routing protocol is the AOMDV routing protocol and is considered for the routing purpose.

2.1.1 Ad hoc On Demand Multipath Distance Vector (AOMDV) Routing Protocol:

AOMDV convention is proposed by marina, it is source activity responsive disjoint multipath directing convention. AOMDV is augmentation of Ad hoc Distance Vector (AODV) directing convention used to locate various disjoint ways in the middle of source and destination. The arrangement (outline) objective behind AOMDV is mistake (shortcoming) resistance from course disappointment for productive and speedier way recuperation. AOMDV utilizes little time out qualities to maintain a strategic distance from rotted (stale) way. 2001

2.1.2 Energy Efficient Multipath Routing Protocol:

A vitality effective multipath directing convention has been proposed by Ke Guan, for remote sensor system. It is unconstrained steering convention. It is in view of the supposition (presumption) of general base station is uprooted and each hub in system may goes about as a source and in addition sink hub. Two trees are given line tree and source tree, in light of the message going in the middle of source and destination course development is finished. The burden of this convention is it telecast the message parcels in system subsequently overhead is expansion. 2004

2.1.3 Low Interference Energy Efficient Routing (LIEMRO) Protocol:

Marjan Radi proposed Low Interference Energy Efficient Routing (LIEMRO) source start up reactive routing protocol. The LIEMRO protocol discovers the multiple paths among source and destination but eliminates the property of node disjointness. The advantage of these protocols is it uses load balancing approach. The load balancing is completed by considering parameters Estimated Transmit Energy (ETX), average residual battery and average interference level for each path. LIEMRO is dissimilar in multipath selection than AOMDV, it do not uses same path once the path is used. Because of special route request packet for each path the overhead of network is increased.

2.1.4 Power Aware Node Disjoint Multipath Source Routing (PNDMSR) protocol:

M. Bhimalingarah proposed a PNDMSR receptive steering convention. It is a source activity steering convention. In PNDMSR just destination hub sends the solicitation bundle to source hub for way revelation. The answer solicitation is shown by source hub in the system. Inadequacy of this convention in distinguishing proof of numerous ways is hard if system is thick.

2.1.5 Secure and Energy Efficient Multipath (SEEM) Routing Protocol:

The (SEEM) steering convention have three sorts of hubs, for example, sensor hub, sink hub and base station hub. The base station acts a vital part in disclosure various ways among the source and the sink hub. The immediate overhead is to a great degree high in the SEEM show as it utilizes Neighbor Discovery (ND) bundle, Neighbor Collection (NC) parcel and Neighbor Collection Reply (NCR) parcel in the directing convention. The ND parcel is transmits in system to recognize the close-by hubs of every hub. Once every hub perceive their contiguous hubs, the base station hub transmit NC parcels with a specific end goal to accumulate the neighbor's data of each node\ gather amid the prior television. The sensor hubs recognize to the NC bundle by sending the neighbor accumulation answer parcel to the base station. The SEEM model legitimizes the security without by the crypto framework gadget in the heading discovering convention.

III. SYSTEM ANALYSIS

Digital Signature:

A Digital signature is an arithmetical strategy used to approve the legitimacy and uprightness of a correspondence, programming or computerized archive. A digital signature method characteristically must have three algorithms;

□ □A key invention algorithm that choose a private key consistently at arbitrary from a situate of probable private keys. The algorithm production the private key as well as a resultant public key.

□ □A signing algorithm that, provide a communication and a private key, generates a
signature.

□ □A signature authenticating algorithm that, specified a communication, public key as well as a signature, or permits or discards the communication preserve to genuineness. Two noteworthy belonging are required. In the first place, the validity of a mark delivered from a perpetual correspondence and changeless private key can be set up by method for the comparable open key. Besides, it must be computationally infeasible to deliver a suitable mark for a customer's lacking important that customer's private key. A computerized mark is a confirmation system that allows the creator of the data to associate a code that works as a mark. It is made by taking the hash of the information and scrambling the information with the producer's private key.

Black Hole Attack:

In attack of black hole, a malevolent node works as a black hole which permits all the movement (traffic) experience (go through) it. In this type of protocol the malevolent node which plays as black hole node reduces the operational of network by continually attacking intentioned node. Subsequent to that malevolent node can place in itself among these communication nodes, among the sink node as well as the source node. The malevolent node can operate whatever thing with the packets as well as every movement (traffic) can justly go through it. This type of attack will permanently obliterate the exacting node by continually attacking on it.

Designing Issue:

1. Independence (autonomy): An supposition of a solitary unit that is taken care of together routing resources and radio networks does not contain any significance in WSN as it is an attack at simple point for network. The routing choices are complete by every nodes in the network than every consolidate node. Therefore the scheming problem of WSN is dissimilar.

2. Battery effectiveness (Energy efficiency): One of the significant problems in WSN, Routing protocols have not utilize huge amount of battery power as preserving a quality link so as to permits interaction among the nodes. Because the criteria of sensor nodes it is infeasible to exchange the nodes battery as they are organized justly one time. Having a few circumstances, the sensors are inaccessible. For example, in wireless subversive sensor network, a few sensor nodes are organized just for sensing the earth.

3. Scalability: The routing protocol must have capability to operate with many numbers of wireless nodes.

4. Fault-tolerant: Sensors have to not quit working unusually as a result of natural reasons or force reason. The Routing conventions ought to manage this inevitability so when a present hub falls flat, an option course have to to be found.

5. Device Heterogeneity: As the greater part of wireless sensor system applications in view of the homogenous hubs however expansion of new sort of hub may be helpful or prerequisite of the applications. The utilization of hubs with heterogeneous handsets, processors, power units or detecting segments may build the execution of the system. Contrasting

and different systems, the heterogeneity of hubs is exceptionally helpful to enhance versatility of the system, the vitality utilization or transfer speed of the wireless sensor network.

6. Mobility Adaptability: Taking into account the application necessity, diverse application may require distinctive normal for the hubs. A few applications obliges portable sink hub, such sort of versatility ought to be given by steering convention.

Security Issue:

Security issues in wireless sensor networks are like the wired system aside from remote qualities of the system. The unguided transmission medium can undoubtedly helpless against assault than guided transmission medium in this way remote systems are effectively inclined to assault. As the remote systems telecast the information in air for remote correspondence hence spying can without much of a stretch happens. Wireless sensor network is a unique instance of remote impromptu system in this manner security issues and strings of remote specially appointed system are like the wireless sensor networks. A few analysts create different techniques to battle against these security issues and strings in remote specially appointed system. Yet, these security systems can't be straightforwardly connected to the remote sensor system in light of the fact that compositional heterogeneity between these two systems. While specially appointed systems are in self-sorting out environment, dynamic topology, shared systems made by a gathering of versatile hubs and in addition the focal thing is not present, the wireless sensor networks may have a train hub or a base station (focal substance communicated as a sink). The outlining qualities of the wireless sensor networks make security component simpler on account of the focal base station. The imperative go up against in remote sensor system is the asset treatment of small sensors. The vast majority of the times it is consider as sensors are sent in perilous territory, for example, once conveyed we can never ready to roll out any improvements in future. In this manner we require a component which can helps us to having secure and true correspondence. Security ought to never must be traded off. A Digital signature is an arithmetical strategy used to approve the legitimacy and uprightness of a correspondence, programming or computerized archive. A digital signature method characteristically must have three algorithms;

□ □A key invention algorithm that choose a private key consistently at arbitrary from a situate of probable private keys. The algorithm production the private key as well as a resultant public key.

□ □A signing algorithm that, provide a communication and a private key, generates a signature.

□ □A signature authenticating algorithm that, specified a communication, public key as well as a signature, or permits or discards the communication preserve to genuineness.

Two noteworthy belonging are required. In the first place, the validity of a mark delivered from a perpetual correspondence and changeless private key can be set up by method for the comparable open key. Besides, it must be computationally infeasible to deliver a suitable mark for a customer’s lacking important that customer's private key. A computerized mark is a confirmation system that allows the creator of the data to associate a code that works as a mark. It is made by taking the hash of the information and scrambling the information with the producer's private key.

Black Hole Attack:

In attack of black hole, a malevolent node works as a black hole which permits all the movement (traffic) experience (go through) it. In this type of protocol the malevolent node which plays as black hole node reduces the operational of network by continually attacking intentioned node. Subsequent to that malevolent node can place in itself among these communication nodes, among the sink node as well as the source node. The malevolent node can operate whatever thing with the packets as well as every movement (traffic) can justly go through it. This type of attack will permanently obliterate the exacting node by continually attacking on it.

Designing Issue:

1. Independence (autonomy): An supposition of a solitary unit that is taken care of together routing resources and radio networks does not contain any significance in WSN as it is an attack at simple point for network. The routing choices are complete by every nodes in the network than every consolidate node. Therefore the scheming problem of WSN is dissimilar.

2. Battery effectiveness (Energy efficiency): One of the significant problems in WSN, Routing protocols have not utilize huge amount of battery power as preserving a quality link so as to permits interaction among the nodes. Because the criteria of sensor nodes it is infeasible to exchange the nodes battery as they are organized justly one time. Having a few circumstances, the sensors are inaccessible. For example, in wireless subversive sensor network, a few sensor nodes are organized just for sensing the earth.

3. Scalability: The routing protocol must have capability to operate with many numbers of wireless nodes.

4. Fault-tolerant: Sensors have to not quit working unusually as a result of natural reasons or force reason. The Routing conventions ought to manage this inevitability so when a present hub falls flat, an option course have to to be found.

5. Device Heterogeneity: As the greater part of wireless sensor system applications in view of the homogenous hubs however expansion of new sort of hub may be helpful or prerequisite of the applications. The utilization of hubs with heterogeneous handsets, processors, power units or detecting segments may build the execution of the system. Contrasting and different systems, the heterogeneity of hubs is exceptionally helpful to enhance versatility of the system, the vitality utilization or transfer speed of the wireless sensor network.

6. Mobility Adaptability: Taking into account the application necessity, diverse application may require distinctive normal for the hubs. A few applications obliges portable sink hub, such sort of versatility ought to be given by steering convention.

Security Issue:
Security issues in wireless sensor networks are like the wired system aside from remote qualities of the system. The unguided transmission medium can undoubtedly helpless against assault than guided transmission medium in this way remote systems are effectively inclined to assault. As the remote systems telecast the information in air for remote correspondence hence spying can without much of a stretch happens.

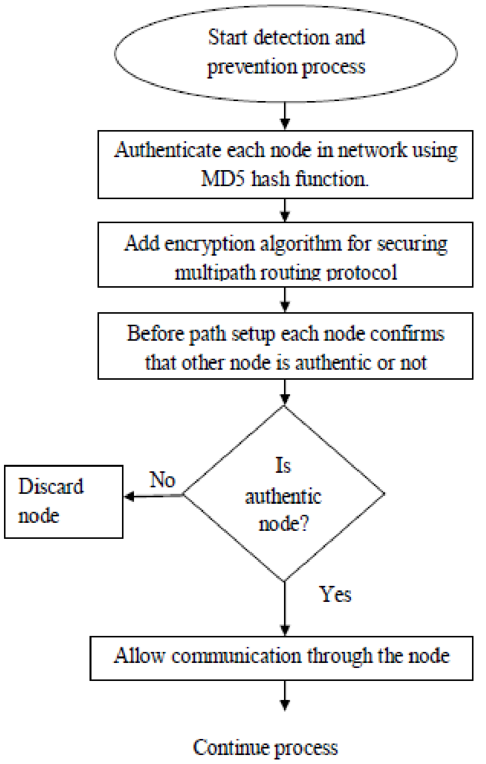
Wireless sensor network is a unique instance of remote impromptu system in this manner security issues and strings of remote specially appointed system are like the wireless sensor networks. A few analysts create different techniques to battle against these security issues and strings in remote specially appointed system.

Yet, these security systems can't be straightforwardly connected to the remote sensor system in light of the fact that compositional heterogeneity between these two systems. While specially appointed systems are in self-sorting out environment, dynamic topology, shared systems made by a gathering of versatile hubs and in addition the focal thing is not present, the wireless sensor networks may have a train hub or a base station (focal substance communicated as a sink). The outlining qualities of the wireless sensor networks make security component simpler on account of the focal base station. The imperative go up against in remote sensor system is the asset treatment of small sensors.

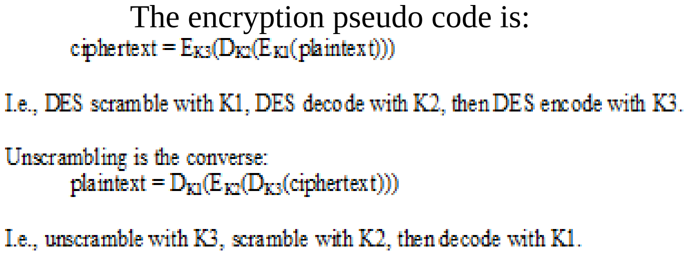
The vast majority of the times it is consider as sensors are sent in perilous territory, for example, once conveyed we can never ready to roll out any improvements in future. In this manner we require a component which can helps us to having secure and true correspondence. Security ought to never must be traded off.

IV. METHODOLOGY

Attack Implantation In black hole assault, a cruel node works as a black hole which allows each movement (traffic) go through it. In this type of the malevolent node which goes about as black hole node aggravate the working of system by always assaulting target node. After that malevolent hub can embed itself between these correspondence hubs, among the sink node and in addition the source node. The vindictive node can do anything with the packets and all the movement can just experience it. This sort of assault can for all time demolish the specific node by continually assaulting on it.
Proposed Scheme


Start detection and prevention process
Authenticate each node in network using MD5 hash function.
Add encryption algorithm for securing multipath routing protocol
Before path setup each node confirms that other node is authentic or not
Is authentic node?
No
Discard node
Yes
Allow communication through the node
Continue process

Triple DES Encryption Algorithm:
Triple DES utilizes a "key package" that contains three DES keys, K1, K2 and K3, each of 56 bits (barring equality bits).


The encryption pseudo code is:

$\text{ciphertext} = E_{K3}(D_{K2}(E_{K1}(\text{plaintext})))$

I.e., DES scramble with K1, DES decode with K2, then DES encode with K3.

Unscrambling is the converse:

$\text{plaintext} = D_{K1}(E_{K2}(D_{K3}(\text{ciphertext})))$

I.e., unscramble with K3, scramble with K2, then decode with K1.

Fig pseudo code for triple DES

Every triple encryption scrambles one piece of 64 bits of information. For every situation the centre operation is the converse of the first and last. This enhances the quality of the calculation when utilizing keying choice 2, and furnishes in reverse similarity with DES with keying alternative 3.

V. CONCLUSION

Wireless sensor networks are susceptible to broad variety of safety halts since of their placing in unsecure and open environment. Here we center on the main safety and scheming problem in WSN and also analysis of the numerous network layer attacks and discovery methods. Researchers improved a numerous discovery and avoidance method for each network layer attack other than there is not every method it is discover out and protect every network layer attack. For discovering such attack types one wants particular safety system apart from presented ones since difficulty of the lack of dispensation, storage and battery power. thus, scheming such security types system is still an open research challenge.