IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 17-21

Dynamic Trust : Trusted Routing Framework In Wsn Against Blockhole Attack And Sinkhole Attacks

Nallakumar R, Preetha Rexlin P.L, Susithra. D, Vickma. S
(Master Of Engineering in Computer Science, Anna University Regional Campus, Coimbatore, Tamil Nadu, India)

Abstract: *The Wireless Sensor Network[WSN] is an infrastructure less, Self-Configuring and dynamic typological oriented Network. The unique features of Wireless Sensor Networks including dynamic topology and open wireless medium, may lead WSN to suffer from many security vulnerabilities. The proposed research deal with the following security issues, such as wormhole, sinkhole attacks, flooding and intrusions. To afford a best possible route for secure data transmission, the system introduces a new secure routing protocol. The new trust based routing protocol "SA-AODV" (Secure Trustable AODV) enables the route discovery with trust calculation mechanism. The trust values have been calculated using two features such as direct trust estimation, and indirect trust observation. Based on the trust, Trust Key Management [TKM] generates and disperses unique security key for all participants, this frequently verifies the keys and authenticates the hops for data transmission. In previous research works, various researchers proposed packet marking techniques to depict and prevent unauthorized access and data misbehaves. But, still those systems are suffering from huge communication overhead due to its huge key size. So, in this proposed Trust Key Managements (TKM) authenticates the hop and data by using small key size. The single bit key verifies the data at every hop and retransmits the key with updated one. Using the key size and route information, the system authenticates every hop in the network.*

Keywords: *Blockhole attack, security trust, Wireless Sensor Network*

I. Introduction

Past few years, have witnessed a rapid escalation in the field of mobile computing due to proliferation of inexpensive, widely available wireless devices. Thus, it has opened vast opportunity for researchers to work on Ad Hoc Networks. In a WSN, nodes within one another's wireless transmission range can communicate directly; however, nodes outside one another's range have to rely on some other nodes to relay messages [1]. Thus, a multi-hop scenario occurs, where several intermediate hosts relay the packets sent by the source host to make them reach the destination node. WSN is one that comes together as needed, not necessarily with any support from the existing infrastructure or any other kind of fixed stations. This statement can be formalized by defining an ad hoc network as an autonomous system of mobile hosts (MHs) (also serving as routers) connected by wireless links, the union of which forms a communication network modeled in the form of an arbitrary communication graph. This is in contrast to the well-known single hop cellular network model that supports the needs of wireless communication by installing base stations (BSs) as access points. In these cellular networks, communications between two mobile nodes completely rely on the wired backbone and the fixed (BSs). In a WSN, no such infrastructure exists and the network topology may dynamically change in an unpredictable manner since nodes are free to move. As for the mode of operation, ad hoc networks are basically peer-to-peer multi-hop mobile wireless networks where information packets are transmitted in a "store-and-forward" manner from a source to an arbitrary destination, via intermediate nodes

The issue of symmetric and asymmetric links is one among the several challenges encountered in a WSN. Another important issue is that different nodes often have different mobility patterns. Some MHs are highly mobile, while others are primarily stationary. It is difficult to predict a MH's movement and pattern of movement [4]. The dynamic nature of WSNs makes network open to attacks and unreliability. Routing is always the most significant part for any networks. Each node should not only work for itself, but should also be co operative with other nodes. WSNs are vulnerable to various security attacks [5]. Hence, finding a secure and trustworthy end-to-end path in WSNs is a genuine challenge. 1.1 Applications of WSN's .The deployment of a WSNs are easy due to the absence of setting up any infrastructure for communication. Mostly such kind of networks is required in military application and emergency rescue operations. But slowly WSNs have entered with the areas of gaming, sensing, and conferencing, collaborative and distributed computing [6]. This dynamic network is yet to capture most of the commercial applications. Research is still going on in this direction so that the WSN can be deployed in any area where a faster and cheaper network can be setup instantly for data communication.

1.2 Applications Of Wsn

1.2.1 Military Services

Military services are one of the most discussed and common application area of Wireless Sensor Networks where installation of any fixed infrastructure is not possible in the enemy territories or inhospitable terrains. In this environment WSN provides the required communication mechanism in no time. Here, the soldiers are considered to be the mobile nodes. So the network is required to remain connected even though the soldiers move freely. This support is provided by the WSN. Another application in this area can be the coordination of the military objects and the personnel in the battlefield. For example, the leader of a group of soldiers may want to pass a message to all the soldiers or a group of soldiers involved in the operation. In this situation, a secure and reliable routing protocol should be able to do the job.

1.2.3 Local Level

Ad-Hoc networks can autonomously link an instant and temporary multimedia network using notebook computers to spread and share information among participants at a e.g. conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information's.

1.2.4 Commercial Sector

E-commerce(anytime and anywhere), inter-vehicle networks as depicted in business(dynamic database access), mobile offices, vehicular services(guidance of road or accident),road and weather conditions transmission, taxi cab network, sports stadiums, trade fairs, shopping malls, networks of visitors inside the airports.

1.2.5 Emergency Services

Sensor network can be wear as search and rescue operations in the desert in the mountain, replacement of fixed infrastructure in case of environmental disasters, policing, fire fighting, supporting doctors and nurses in hospitals

II. Review Of Literature

2.1 Mobile Target Detection In Wireless Sensor Networks

The important issue of the balance between the quality of target detection and lifetime in wireless sensor networks. Two target-monitoring schemes are proposed. One scheme is Target Detection with Sensing Frequency K (TDSFK), which distributes the sensing time that currently is only on a portion of the sensing period into the entire sensing period. That is, the sensing frequency increases from 1 to K. The other scheme is Target Detection with Adjustable Sensing Frequency (TDASF), which adjusts the sensing frequency on those nodes that have residual energy. The simulation results show that the TDASF scheme can improve the network lifetime by more than 17.4% and can reduce the weighted detection delay by more than 101.6%. The unequal sensing frequency in different regions is used to improve the monitor quality by taking the advantages of the residual energy throughout the network. The second scheme provides the method for the calculation of proper frequency value. The evaluation of the performances of the proposed schemes was made with three parameters: probability of missed target, delay, and lifetime. Computer simulation results show that the TDASF scheme can improve the network lifetime by more than 17.4% and can reduce the weighted detection delay by more than 101.6%. The algorithm proposed in this paper is for the static sink WSNs.

2.2 An Eficient Heuristic Subtraction Deployment Strategy

Cooperative sensing and monitoring event is one of the important applications of sensor networks. Node deployment and duty cycle configuration of event detection in a large wireless sensor networks is an enormous challenge. Through in-depth analysis we find that there is a tradeoff between node duty cycle and event quality monitoring. That is, adopting larger duty cycle enables network to deploy fewer nodesOr deploying more nodes can reduce their duty cycle. Both of them can reach the event detecting quality requirement of application. Based on the above findings, a novel subtraction deployment strategy (SDS) combined with the unequal node duty cycle in the network is presented. SDS guarantees the quality of event detection needed for the application by reducing the number of nodes and improving the sensing duty cycle in the areas of low energy consumption. This paper reveals the optimization relationship among node density, sensing duty cycle and detection quality for the first time, and gives the solving model of optimization. We find that the above optimization solution is a very complex nonlinear relation, therefore, a heuristic optimization algorithm is proposed to solve subtraction deployment problem.

2.3 Differential Game-Based Strategies

A game-theoretic approach to limit malware in WSNs. Epidemic theory has been developed and a malware propagation model satisfying the characteristics of sensor nodes has been constructed under the consideration of effort intensities of the system and malware. We have solved, by formulating a malwaredefense differential game, the contradiction between achieving QoSguaranteed communications and minimizing the interference generated due to employing security methods. Experimental results have shown that our model closely matches the simulation, which indicates our approach can help the system attain the optimal dynamic strategies when the malware dynamically changes its strategies. These strategies are able to evidently suppress the propagation of the malware and are convenient to be applied to sensor nodes. Besides, the other potential application of our approach may exist in social networks, due to the similarity that social networking accounts may sleep when the user logs out. . One typical example using signal-processing techniques is a topologically aware worm propagation model , which can simultaneously capture the worms' time and space dynamics. More typical examples are based on epidemic theory, whose successful applications include worm modeling, fault propagation, and epidemic algorithms for the spread of information; these epidemic frameworks, and have some deficiencies in reflecting characteristics of sensor nodes.

2.4 Ids Model To Enhance The Security In The Aodv

In this scheme, each node employs an IDM that uses neighborhood information to detect misbehavior of its neighbors. When the misbehavior count of a particular neighbor reaches a predefined threshold, the information is sent to other nodes. When a node receives this information, it checks the local misbehavior count for the malicious node and adds its result to the initiator's response. Cooperation of Nodes Fairness in Dynamic Ad-hoc Network (CONFIDANT) developed is an extended version of Watchdog and Pathrater. Unlike Watchdog and Pathrater, this scheme punishes the misbehaving nodes. Nodes with bad reputation are isolated in order to limit their activity in the network. Thus CONFIDANT, unlike Watchdog and Pathranter, stimulates misbehaving nodes from contributing to the normal operations of the network. The optimal strategy, different control methods have been adopted. Using Pontryagin's maximum serially found optimal solutions, including optimal quarantining of malware optimal dissemination of security patches maximum damage malware attack and maximum damage battery depletion attack

III. Existing System

Existing authentication routing protocol in WSNs can be mainly classified into two categories: hop-by-hop authentication and detection based approaches. Some excellent work has been proposed on detection based approaches based on trust in WSNs. The most existing approaches do not exploit direct and indirect observation at the sometime to evaluate the trust of an observation node. In indirect observation in the most approaches is only used to assess the reliability of node, which are not in the range of the observer node. The inaccurate trust value many be derived. In this method, trust evaluation from direct observation do not differentiate date packet and control packet. The control packet usually are more important than data packet

IV. Problem Statement

The WSN is very easy to use and at the same time, it is also cost effective one. But, its infrastructure less Environment paves way for challenging security problems. The most important problems in WSNs are secure routing in presence of selfish or adversarial entities which drop the packets they agreed to forward; and in doing this selfish or adversarial entities can disrupt the network traffic and cause various communication problems, Wormhole attack which access data illegally, flooding packets and making the network to vast working time. Several research works have been proposed to provide secure route discovery and detection and prevention of attacks. Each one has its own limitations and constraints. Many existing solutions address ways to provide security using cryptography and/or trust based security are presented in the literature covered.

V. Proposed System

Secure data transmission in WSN is a challenging task due to its wide variety of attacks. As per the previous discussion on chapter 2, there are several types of attacks interrupts data transmission in Ad hoc networks, but only few algorithms and protocols have been developed to get rid of those attacks. In order to provide secure routing and data authentication, the proposed work has been introduced. Recently, key management is observed to provide better results on the security against those attacks. These key management schemes can protect the data and authenticates group communications. But, the major problem of key management in the ad-hoc network is the security of the group communication. This research proposes a new trust based protocol for effective secure route discovery of WSN.

Many protocols have been designed and implemented to provide secure routing and data transfer, which ultimately results in too much overhead and routing load in the network. Keeping this in view, the **ST-AODV** is proposed and implemented to eliminate unwanted computational and processing overheads that degrade the network. The **ST-AODV** provides a good packet delivery ratio by choosing highly secure nodes, based on trust to establish an authenticated route, thereby enabling secure data transfer.

- A new trust management scheme which protects the data from sinkhole, intrusion and man in middle attacks has been proposed.
- Proposes a lightweight single bit key based packet marking technique for fast attack detection. The key generation is created.

VI. Architecture Diagram

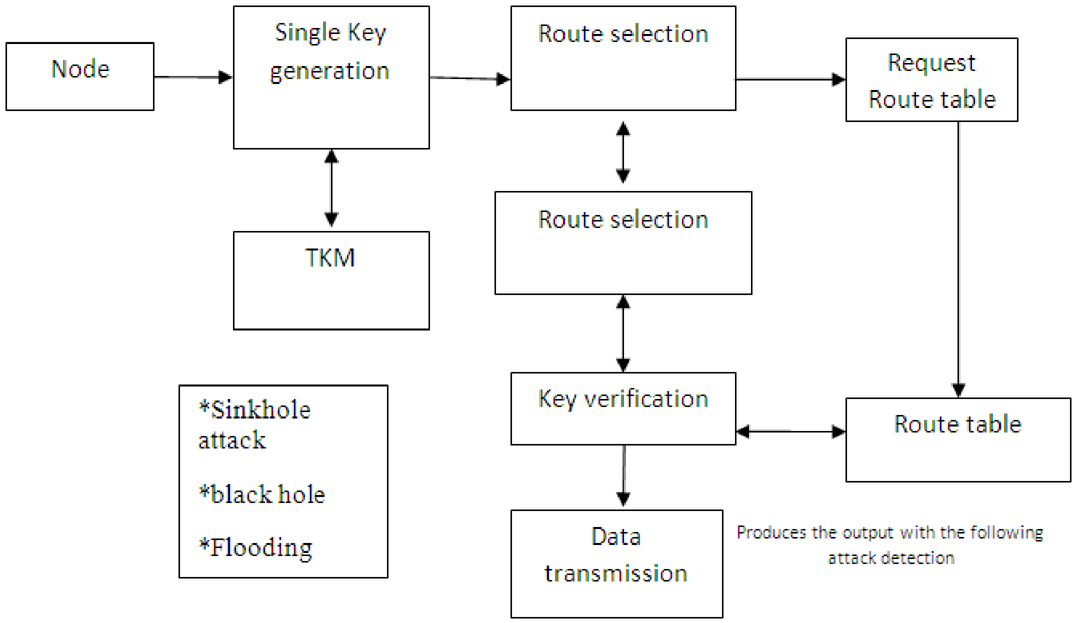

Fig 6.1 Overall Architecture of Proposed System

VII. Modules Description

7.1 Network Construction

The first module is initial network construction with 50 mobile nodes. The system simulated the proposed scheme by using the ns-2 network simulator. In the simulation, 50 mobile nodes are placed within a square area of 1500 m × *1*500 m. this use Random Mobility model to determine movements of mobile sensor nodes. In the Random mobility model, each node moves to a randomly chosen location with a randomly selected speed between a predefined minimum and maximum speed. After reaching that location, it stays there for a predefined pause time. It then randomly chooses another location after that pause time and moves to that location. This random movement process is repeated during a simulation time.

7.2 Attacker Model

The attacker model simulates the data replacement attacks by anyone of the node in the list. The application is created with random node selection for performing the attacks. The data replacement attacks will be performed by a random node, based on this scenario, the attack will be simulated.

7.3 Ecdsa Algorithm Implementation

The system performs ECDSA based encryption scheme for secure data transmission. This helps to prevent the data from attack. The second module creates an authentication key based on node analysis. In the key generation process, keys are generated dynamically using local time and neighbor details. The ECDSA algorithm works one public and private key system. The public key is made available to everyone. With this key a user can encrypt data but cannot decrypt it, the only person who can decrypt it is the one who possesses the private key. It is theoretically possible but extremely difficult to generate the private key from the public key, this makes the ECDSA algorithm a very popular choice in data encryption.

7.4 Neighborhood Monitoring And Voting Process

This module proposes a mechanism to detect any control or data attack that results from dropping, delaying, modifying, or fabricating of packets. This module allows a node to distinguish between its neighbors to prevent identity spoofing among them. This is used to build a data structure of the first-hop neighbors of each node and the neighbors of each neighbor. The data structure is used in local monitoring to detect malicious nodes and in local response to isolate these nodes. The message receiver should be able to verify whether a received message is sent by the node that is verified or by a node in a particular group. The adversaries cannot pretend to be an innocent node and inject fake messages into the network without being detected. The proposed message authentication scheme performs a single bit key updating and appending process. The main idea is that for each message *m* to be released, the message sender, or the sending node, generates a source message authenticator for the message *m*. The generation is based on the novel SBK (single bit key) scheme on ECDSA .

7.5 Trust Calculation And False Information Filtering

Finally the false data will be filtered and malicious node will be blocked based on the key identification. If the key size is greater than the threshold, then the data has been considered as malicious. The data will be dropped further.

VIII. Conclusion

The system proposed a new secure trust based routing protocol named as SA-AODV protocol against different type's attacks in the WSN such as flooding attacks, wormhole attacks and sinkhole attacks. Especially, the approach effectively prevents the data from potential damages due to data attackers and this also protects data by using modified ECDSA cryptographic function. In order to measure the risk of attacks and data authentication at each hop has been carried out with single bit key verification. This system extended the work of pinpointing the attacker node to their neighbors. Based on several metrics, this system is investigated the performance and other security approach and the experiment results clearly demonstrated the effectiveness and scalability of this proposed SA-AODV mechanism approach.

References

1. Dallas, Daniel, Christopher Leckie, and KotagiriRamamohanarao,(2007) "Hop count monitoring: Detecting sinkhole attacks in wireless sensor networks".
2. Krontiris, Ioannis, ThanassisGiannetsos, and TassosDimitriou,(2008) "Launching a sinkhole attack in wireless sensor networks; the intruder side." Networking and Communications, WIMOB'08. IEEE International Conference on Wireless and Mobile Computing,.
3. LiuA,Dong M, Ota K, et al(2015) "An Efficient Scheme for Selective Forwarding Attack Detecting in WSNs,"
4. Liu A, Jin X, CuiG,Chen Z,(2013) "Deployment guidelines for achieving maximum lifetime and avoiding energy holes in sensor network," Information Sciences.
5. Macker, Joseph. (1999)"Wireless Sensor Networking (WSN): Routing protocol Performance issues and evaluation considerations.
6. Maliyah, Likes, Achilles A. Woo, and Sanjay Sharma,(2013) "New Load Balanced Multi-Path Dynamic Source Routing Protocol for Wireless Sensor Network." International Journal of Computer Applications.
7. Onate, Liker, and Ali Miri,(2005) "An intrusion detection system for wireless SensorNetworks. "Wirelessand Mobile Computing, Networking and Communications.
8. Royer, Elizabeth M., and Chai-KeungThough,(1999) "A review of current routing Protocols for ad hoc mobile wireless networks." Personal Communications.
9. Shu K,Runs M, Liu S,(2010) "Secure data collection in wireless sensor networks Using randomized dispersive routes," IEEE Transactions on Mobile Computing.
10. Srinivasan, Vanish, et al,(2009) "Reputation-and-Trust-Based Systems for AdHoc Networks." Algorithms and protocols for wireless and Wireless Sensor Networks.