Wireless Sensor Network Security Using Cryptography by Modified AODV with Diffie-Helman & Hash Algorithm

[1]Manisha Ingale, [2]Surabhi Tankkar

[1]Student, [2]Assistant Professor
[1, 2]M.E Electronics & Telecommunication Engineering,
AlamuriRatnamala Institute of Engineering and Technology,
Shahpur, Asangaon, India

***Abstract*: In ad hoc networks, each node in the network must be able to take care of routing of the data and this is the domain of ad-hoc routing. As often pointed out, routing is a critical issue for ad-hoc networks while it has certainly been addressed extensively by the research community. This system addresses some issues pertaining to mobile ad-hoc networks due to lack of infrastructure and dynamic topology. The mobility of these nodes imposes issues in terms of mobility management, energy consumption, battery life and security. Thus, there is need to optimize these parameters with minimum cost for designing routing protocol. In the system, comprehensive review of existing routing protocols and their issues have been studied in detail [1]. To provide secure routing in ad-hoc networks, it is essential that each node should be authentic. The presence of malicious nodes in an ad-hoc network deteriorates the network performance. In this system, new algorithms are proposed to mitigate the problem of malicious node.**

***Index Terms*: Cryptography, Diffie-Helman, AODV, RSA.**

1. INTRODUCTION

1.1 AODV

Reactive protocols seek to set up routes on-demand. If a node wants to initiate communication with a node to which it has no route, the routing protocol will try to establish such a route. AODV is on-demand source routing scheme that combines the features of Dynamic Source Routing (DSR) and Destination Sequenced Distance Vector (DSDV) routing schemes. AODV adapts the route maintenance and route discovery mechanism of DSR. The use of sequence number to avoid loops and minimum hop routing is adapted by AODV from DSDV. AODV offers fast adaptation to link changes. Because of minimum hop routing and has low traffic overhead because of its reactive nature. When the source node has a packet to send to a destination node, it first checks for the valid route to that destination if there exists a valid route then the packet is sent. If the valid route does not exist, the node initiates a route discovery process by broadcasting Route Request (RREQ) packets to its neighbours. The receiving nodes of the RREQ packets other than destination and intermediate node having a fresh entry to the destination rebroadcasts the RREQ packet. The area of RREQ dissemination is reduced through the use of expanding ring search technique [2]. Time to Live (TTL) field is used to control the dissemination of the RREQ packets. When the hop count is reached the limit indicated by TTL field, the intermediate node simply drops the packet instead of rebroadcasting it.

1.2 AOMDV

Ad hoc On-demand Multipath Distance Vector (AOMDV) is the enhanced version of AODV protocol, it belongs to on demand and reactive routing protocol of ad-hoc wireless networks. The main goal is to compute multiple loop-free and link-disjoint paths between source and destination pair. The merit of AOMDV is estimated in terms of increased packet delivery ratio, throughput and reduced average end-to-end delay and normalized control overhead. The average end to end delay is reduced by introducing multiple loop free paths in this scheme. In multiple routes, the destination contains list of the next-hops along with the corresponding hop counts in routing table entries. Suppose all the next hops have the same sequence number. The advertised hop count is defined as the maximum hop count for all the paths. Route advertisement sends to destination by using this hop count value. If any duplicate route advertisement received by a node then it forwards the packet thro alternate path to the destination. The RREQ and RREP pair arrives through different neighbour of the source in a node-disjoint path. During route discovery, the source node broadcasts a ROUTE REQUEST packet that is broadcasted throughout the network. In contrast to AODV, each recipient node creates multiple reverse routes while processing the ROUTE REQUEST packets that are received from multiple neighbours.
AOMDV is based on the distance vector concept and the hop-by-hop routing approach is used here. Several RREPs traverse through these reverse paths back to the source node to create multiple forward paths to the destination at the source as well as at intermediate nodes.
The AOMDV route discovery process consists of two modules:

1. A route update rule is used to establish and maintain multiple loop-free paths at each node and
2. A distributed protocol to find link-disjoint paths.

When a route is required, the source broadcasts the RREQ for the destination throughout the network. A node which receives the RREQ checks the destination field of RREQ packet [3]. If the node itself is the destination or if it has routing information for the destination node, it replies and sends the RREP packet to the sender. If no routing information is available it will send RERR message to the sender.

2. LITRATURE REVIEW

For the most part, security issue in steering convention has not given much consideration, since the majority of the directing convention in WSNs has not been created in view of security. Numerous progressive directing conventions have been created, where vitality effectiveness is the principle objective. In numerous applications like military and war zone, information is significant and need to keep up mystery in information correspondence between sensor hubs and BS. Security is an entrenched field for universally useful figuring where security systems address registering administrations like verification, interruption location and give secure exchange. Since the battery life limits the lifetime of a sensor hub, control utilization is typically set as the principal need in creating security arrangements. Sensor systems are sent in an unfriendly domain, security turns out to be critical as these systems are inclined to various sorts of malignant assaults. To give security, correspondence exchanges ought to be scrambled and verified. Symmetric key plan is progressively proper cryptography (SKC) for remote sensor organizes because of its low vitality utilization and straightforward equipment prerequisites; however the greater part of them can't give adequate security level as open key cryptography like respectability, classification and verification. Cryptographic natives are the premise of security arrangements and the most habitually executed security tasks in sensor systems. Cryptography is the specialty of accomplishing security by encoding messages to make them non-comprehensible. Cryptography is the investigation of concealing data that empowers to store touchy data and furthermore transmit it crosswise over unreliable systems yet it can't be perused by anybody aside from the expected beneficiary. Symmetric calculations, the two gatherings share a similar key for encryption and unscrambling.

Some networks have the abilities of being not connected to a central node, self-managing and healing, not being connected to a specific network topology, multi-way routing, preserving the integrity and confidentiality of data, and being robust. Today's on-going work: designing sensors that are resistant to harsh weather conditions, reducing energy consumption, designing low-cost sensors with high capacities, and making data flow faster and safer. The data obtained from the sensors must be transmitted safely to the target. Wireless sensor networks have a large number of attack types (Sybil, Wormhole, Sinkhole, etc.) that threaten data flow. While designing security policies, a general structure is aimed at eliminating some or all of the attacks. For this reason, policies based on information security principles such as privacy; integrity, availability, authentication and non-repudiation have been developed [4].

The RSSI method is first improved is improved by using the median weighting method so as to improve the range precision of the nodes. To further improve the localization accuracy of the nodes, a three-dimensional node localization model is established based on the least square support vector regression method. Lastly, a detection mechanism against sybil attacks is presented to improve the security of localization against sybil attacks. The simulation results show that the accuracy and safety of the improved localization algorithm are better than the traditional localization algorithm [5]. Wireless Sensor Network is the combination of small devices called sensor nodes, gateways and software. These nodes use wireless medium for transmission and are capable to sense and transmit the data to other nodes. Generally, WSN composed of two types of nodes i.e. generic nodes and gateway nodes. Generic nodes having the ability to sense while gateway nodes are used to route that information. IoT now extended to IoET (internet of Everything) to cover all electronics exist around, like a body sensor networks, VANET's, smart grid stations, smartphone, PDA's, autonomous cars, refrigerators and smart toasters that can communicate and share information using existing network technologies. The sensor nodes in WSN have very limited transmission range as well as limited processing speed, storage capacities and low battery power [6].

Wireless Sensor Networks (WSNs) are designed with hundreds and thousands of sensor nodes that are operated in an unsecured or in hostile unattended environment. Since these networks have wide applications in military, health monitoring areas, industrial processing, ocean & wildlife monitoring, etc., requires the interaction with sensitive data yields the biggest challenge to provide security in routing protocols. Along with the security, WSNs have some other constraints such as physical capture, energy consumption, low capacity, etc. To overcome the above constraints, it is required to design an efficient Wireless Sensor Network that consumes less power, small in size and highly secured. To achieve the required objective, here they have modified the R-XOR algorithm by adding some more features to increase its efficiency. The proposed algorithm is analyzed and proved that the throughput is high and overhead is reduced by comparing with existing R-XOR algorithm. [7]. In New Security Protocol using Hybrid Cryptography Algorithm for WSNDOI aims to propose a hybrid security protocol for WSN [8].

The Software-Defined Wireless Sensor Networking (SDWSN) paradigm aims to solve inherent issues present in Wireless Sensor Networks (WSN), such as resource constraints, by adopting a Software-Defined Networking (SDN) approach to the management of these WSNs. The security aspect of SDWSN has received little attention due to a focus on the architecture. As this paradigm is a combination of both WSN and SDN, some solutions from both paradigms can be adapted to consider SDWSN. One of the main problems with implementing security within WSN, lies within its inherent issues, such as resource constraints. However, due to the centralization of control brought about by the SDN paradigm, most of these issues are alleviated, leaving room for WSN security implementations. In order to investigate the use of WSN cryptography within SDWSN, cryptography methods have been implemented within a SDWSN network in order to verify whether the SDWSN paradigm does allow for resource intense WSN security implementations [9]. Wireless sensor network (WSN) is a collection of various sensor nodes. These sensor nodes sense data from the surrounding and send it to its destination following a proper route. A sensor network has various applications to monitor physical phenomenon in military, agriculture and medical applications where it can be used to make human life better in many ways. There are many issues in WSN [10].

The intent of this paper they point out that the operating frequency could be a significant factor influencing the overall power consumption of a target security solution, which has been unnoticed before. Based on this finding a novel concept is proposed to optimize the security solution in terms of power. An empirical platform is setup on top of FPGA devices to investigate the feasibility of this idea in practice. This study concludes that a further power optimization can be obtained by adjusting operating frequency even though implementing hardware and programming technique are fixed for a particular security [11]. In this paper they conducted a simulation-based CPA attack on AES implementations with different S-box structures. Our results show that the abilities of AES and S-boxes to secure against CPA attack are correlated, and an evaluation of the ability of S-boxes to thwart CPA is presented in a quantitative way. By further exploiting, a novel byte substitution circuit used inhomogeneous S-boxes instead of fixed S-boxes was proposed, and the simulation result shows that power consumption becomes randomized and the peak corresponding to the correct key is masked successfully [12].

Attack Detection and Localization Scheme (ADLS) to detect and localize the identity-based attacks. An improved algorithm for hashing has also been proposed. They named it as Effective Hashing Technique (EHT). It generates the Hash keys to differentiate an attacker from a normal node and to reduce the occurrences of any false positives or negatives. Also, our localization algorithm efficiently finds out the position estimates for the nodes. With the help of this method they can robustly identify the adversaries and localize them to prevent further large scale network malicious attacks like DoS and resource depletion attacks. They present simulation for 802.15.4 (Zigbee) based real time home security system and analyse its performance based on NS2 [13]. The intent of this paper is to provide structured and comprehensive study of prominent security attacks reported in the literature for mobile ad hoc networks. In addition, They also discuss various well-known reactive and proactive security solutions proposed in literature to prevent those attacks in MANETs. Finally, the paper is concluded with a brief discussion on future direction of research in MANETs [14].

3. ALGORITHM

3.1 Hash Algorithm

Hash algorithms play an important role in modern cryptography. They are widely used in a variety of security applications such as node authentication, message authentication, password protection, digital signature etc. The hash function uses a string of arbitrary length as its input and creates a fixed-length string as output. The fixed-length hash value is often called message digest. The most widely used hash functions are one-way functions for which finding an input which hashes to a pre-specified hash-value is very difficult. Hash functions may be split into two classes: unkeyed hash functions, whose specification dictates a single input parameter (a message); and keyed hash functions, whose specification dictates two distinct inputs, a message and a secret key. Two commonly used functions are MD5 and SHA-1. Both SHA-1 and MD5 are derived from MD4 which has been known for its weaknesses. MD5 which uses a hash algorithm with 128-bit output has been designed in 1991 and in 2005 it was shown how quickly random collisions for MD5 can be constructed. Also, it is not suitable for applications that rely on the properties like SSL certificates or digital signatures. In authors have shown that how a pair of X.509 certificates can be created that result in the same MD5 hash digest [15]. Then cryptographers began recommending the use of other algorithms, such as SHA-1 which has since been found to be vulnerable as well and most U.S. government applications now require the SHA-2 and SHA-3 family of hash functions. But most of these widely used hash functions are used in large conventional networks.

3.2 Diffie-Helman Algorithm

Diffie-Hellman is an important method of exchanging the keys between two parties. It is an earliest example of key exchange implemented within field of cryptography. That shared secret key can be used to encrypt the information using a symmetric key cipher. The Diffie-Hellman algorithm is used to generate the public key. The symmetric public key algorithm exchanges the secret key between two users over an insecure channel without any prior knowledge. The Diffie Hellman functionality is limited to key exchange only. Diffie-Hellman key exchange algorithm cannot be used for encryption and decryption and it does not provide any type of authentication between two parties. Diffie-Hellman algorithm main disadvantage is that it is vulnerable to man in the middle attack In present algorithm, time complexity and analysis will be measured as well as Diffie-Hellman key will be used for encryption and decryption using proposed algorithm. The RSA and Diffie Hellman key exchange protocol are public key encryption algorithms that are used for commercial purposes. The minimum needed key length for encryption and decryption systems is 128 bits, although both algorithms use 1024-bit keys. Both algorithms were introduced in the 1970 and have to be cracked.

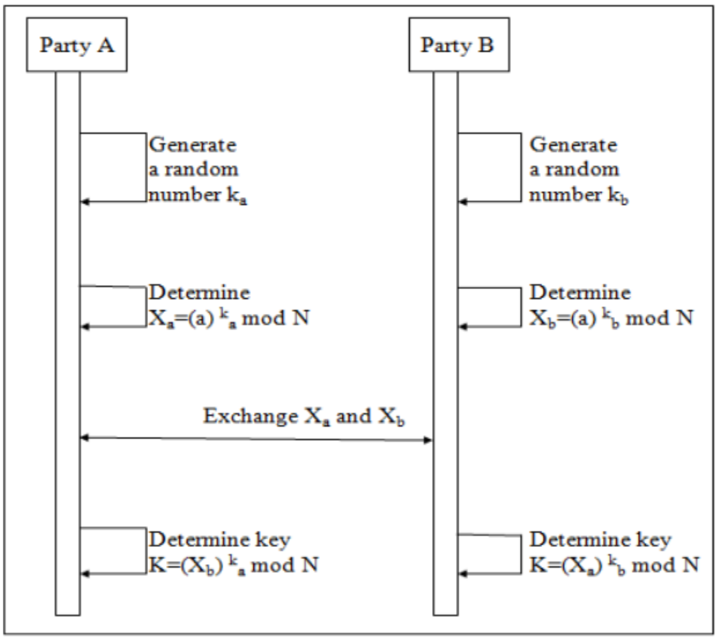
Party A
Party B
Generate a random number k_a
Generate a random number k_b
Determine $X_a=(a)^{k_a}$ mod N
Determine $X_b=(a)^{k_b}$ mod N
Exchange X_a and X_b
Determine key $K=(X_b)^{k_a}$ mod N
Determine key $K=(X_a)^{k_b}$ mod N

Fig. 3.2: Key Exchange by using DIFFIE HELMAN

4. PROPOSED METHODOLOGY

In the proposed work, AODV has been used and various modifications are proposed in that. When P is not the destination node it further broadcasts the packet to its neighbour. P sets up a reverse route entry in its route table for the source S. The entry contains the IP address and current sequence number of S, number of hops to S and the address of the neighbour from whom P got the RREQ. Now we add another fields that are the node id of neighbour to which P forwards RREQ, sending time of P, receiving RREQ time of P‘s neighbour and count. Count is the difference of sending and receiving time.

We use the concept of encryption and uses Diffie-Helman algorithm and Hash Algorihtm. This encryption provides security from attacker nodes. In route reply packet, we add additional field for Diffie-Helman algorithm. When a destination node forwards RREP packet, each node through which the RREP is unicasted performs the decryption to check the authenticity of the packet

4.1 System Assumptions

At the link layer, it assumes that a node can always monitor ongoing transmissions even if the node itself is not the intended receiver.

- We also assume that radio links are bi-directional; that is, if a node A is in transmission range of some node B, then B is in transmission range of A.
- We further assume that the transmission range of an attacker node is similar to a normal node because more powerful transceiver is easy to detect.

4.2 Advantages of Integrating Our Modified AODV With RSA Encryption

- We have a kind of double verification, one is through our RREQ packet and other is through Diffie-Helman encryption algorithm.
- Removal of false nodes in the network.
- We come to know the exact location of attacker nodes.
- Using modified AODV i.e. EAODV with multipath routing by introducing no. of hops and Diffie Helman encryption, we propose secure and energy optimized routing algorithm based on multiple path in wireless sensor networks.

5. WORMHOLE DETECTION MECHANISM

5.1 Sending smart packet & Processing Request

The smart packet is send to the neighbouring nodes up-to two hops. This packet is supposed to be dropped by the authorized nodes. But if this packet is resend by any node, that node is supposed to be malicious and that node is to be checked further for confirming that the node is actually malicious.

5.2 Conformation

- First Process*:* When a node receives such a processing request, it will check its own table and if the same pattern exists, it will reply as true to the requesting node.
- Second Process*:* the nodes at the two ends of wormhole send some encrypted messages to one another. Every privileged node on the path can be able to process those messages (we assume colluding nodes cannot decrypt and hence cannot process) and will add their signatures/stamps/flag to the encrypt packet pay load.

- Third Process*:* When a destination node receives the encrypted message, it will look for signatures of all nodes along the path, if every node has added its signature to the encrypted payload; it will consider it as normal. If the signature of any node along the path is missing, it will consider it as a wormhole

5.3 Prevention Mechanism

- Blacklist of Malicious Node: When the source node receives the encrypted reply and the wormhole existence is confirmed, we need to cut-off the malicious nodes so that no further communication takes place with them and hence they are black listed.
- Alert Generation & Communication: Upon the confirmation of wormhole, both end nodes broadcasts a blacklisting message. This message contains list of malicious nodes to be excluded from communication and not to entertain any path update or any future request from them.

5. CONCLUSION

Wormhole attack in WSNs has been drawing more and more attention since it can disrupt normal network routing protocols. However, in previous work of wormhole detection, most of them need either extra hardware or clock synchronizations and suffer from high complexity. In view of the discovering results and examination, both AODV and AOMDV steering conventions are powerless against dark gap assaults in VANETs condition. Despite the fact that the distinctions are not huge, the AOMDV organize execution is superior to AODV. It is on the grounds that the AOMDV directing procedure utilizes multipath contrasted with AODV which just gives unipath. Because of the dark gap assaults intends to upset the accessibility of system benefits, the ease of use of multipath steering would be a superior choice to keep away from the malevolent hub information bundles assimilation. The future work of this exploration will concentrate on the improvement of AOMDV security by changing the directing convention calculation. Since AOMDV is a multipath steering convention that using all accessible way to transmit the information bundles, the security improvement of AOMDV directing convention could distinguish and avert the aggravated of system accessibility from the noxious hubs as ahead of schedule as would be prudent. The safe AOMDV directing convention will give the careful elective ways to convey the information parcels from their source to the goal without the disturbance from any aggressor competitors.

REFERENCES

[1] Mounika Tokala ; Rajeswari Nallamekala "Secured algorithm for routing the military field data using Dynamic Sink: WSN"DOI: 10.1109/ICICCT.2018.8473343IEEE 2018.

[2] S. Malathy ; J. Geetha ; A. Suresh ; S. PriyaImplementing Elliptic Curve Cryptography with ACO Based Algorithm in Clustered WSN for Border Surveillance.

[3] A. P. Renold, R. Poongothai, and R. Parthasarathy, "Performance analysis of LEACH with gray hole attack in Wireless Sensor Networks," in International Conference on Computer Communication and Informatics, 2012, pp. 1–4

[4] Aykut Karakaya ; Sedat Akleylek " A survey on security threats and authentication approaches in wireless sensor networks"2018 IEEE INSPEC Accession Number: 17737378 DOI: 10.1109/ISDFS.2018.8355381.

[5] Lieping Zhang ; Huanhuan Yang ; Yanlin Yu ; Fei Peng Electronic A Three-Dimensional Node Security Localization Method for WSN Based on Improved RSSI-LSSVR Algorithm 2018 IEEEISSN: 2157-1481INSPEC Accession Number: 17715536DOI: 10.1109/ICMTMA.2018.00051

[6] Shoukat Ali ; Muazzam A Khan ; Jawad Ahmad ; Asad W. Malik ; Anis ur RehmanDetection and prevention of Black Hole Attacks in IOT &amp; WSNINSPEC Accession Number: 17805441 IEEE 2018DOI: 10.1109/FMEC.2018.8364068

[7] B. AnandaKrishna ; N. Madhuri ; M. Koteswara Rao ; B. VijaySekar Implementation of a novel cryptographic algorithm in Wireless Sensor NetworksIEEE 2018INSPEC Accession Number: 17632791DOI: 10.1109/SPACES.2018.8316335

[8] Khalid M. Abdullah ; Essam H. Houssein ; Hala H. Zayed New Security Protocol using Hybrid Cryptography Algorithm for WSNDOI: 10.1109/CAIS.2018.8442003

[9] Sean W. Pritchard ; Gerhard P. Hancke ; Adnan M. Abu-Mahfouz Cryptography Methods for Software-Defined Wireless Sensor NetworksElectronic ISSN: 2163-5145INSPEC Accession Number: 18025222DOI: 10.1109/ISIE.2018.8433630

[10] Rajendra Kumar Dwivedi ; Prachi Sharma ; Rakesh KumarDetection and Prevention Analysis of Wormhole Attack in Wireless Sensor Network

[11] Xiao Xiong , Steve Hill : "The Impact of Operating Frequency on Power Optimization for Wireless Sensor Networks Security" IEEE 17 November 2009 ISBN: 978-0-7695-3786-3

[12] Zhaoxia Zheng ; Xuecheng Zou ; Zhenglin Liu ; Yicheng Chen "Security Analysis and Optimization of AES S-Boxes Against CPA Attack in Wireless Sensor Network" 2007 International Conference on Wireless Communications, Networking and Mobile Computing, 08 October 2007 IEEE.

[13] Ulya Sabeel ; Nidhi Chandra ; Shivraj Dagadi A Novel Scheme for Multiple Spoof Attack Detection and Localization on WSN-based Home Security System, 2013 5th International Conference and Computational Intelligence and Communication Networks, IEEE 11 November 2013

[14] M. O. Pervaiz, M. Cardei, and J. Wu, "Routing security in ad hoc wireless networks," in Network Security, S. C.-H. Huang, D. MacCallum, and D.-Z. Du, Eds. Boston, MA: Springer US, 2010, pp. 117–142

[15] W. Zada Khan, Y. Xiang, M. Y Aalsalem, and Q. Arshad, "The Selective Forwarding Attack in Sensor Networks: Detections and Countermeasures," International Journal of Wireless and Microwave Technologies (IJWMT), vol. 2, no. 2, pp. 33–44, Apr. 2012.