CONCEALED DATA AGGREGATION WITH DYNAMIC INTRUSION DETECTION SYSTEM TO REMOVE VULNERABILITIES IN WIRELESS SENSOR NETWORKS

Bharat Bhushan[1], Keshav Kaushik[2] and G Sahoo[3]

[1,3]Department of Computer Engineering, BIT Mesra, Ranchi, India
Bharat_bhushan1989@yahoo.com
gsahoo@bitmesra.ac.in
[2]Department of Computer Engineering, HMRITM, New Delhi, India
Keshavkaushik96@gmail.com

ABSTRACT

Data Aggregation is a vital aspect in WSNs (Wireless Sensor Networks) and this is because it reduces the quantity of data to be transmitted over the complex network. In earlier studies authors used homomorphic encryption properties for concealing statement during aggregation such that encrypted data can be aggregated algebraically without decrypting them. These schemes are not applicable for multi applications which lead to proposal of Concealed Data Aggregation for Multi Applications (CDAMA). It is designed for multi applications, as it provides secure counting ability. In wireless sensor networks SN are unarmed and are susceptible to attacks. Considering the defence aspect of wireless environment we have used DYDOG (Dynamic Intrusion Detection Protocol Model) and a customized key generation procedure that uses Digital Signatures and also Two Fish Algorithms along with CDAMA for augmentation of security and throughput. To prove our proposed scheme's robustness and effectiveness, we conducted the simulations, inclusive analysis and comparisons at the ending.

KEYWORDS

Concealed Data Aggregation, Digital Signatures, DYDOG, Wireless Sensor Networks.

1. INTRODUCTION

WIRELESS sensor networks (WSNs) have gained much significance in past few years because of its huge number of applications and areas of use. The application domain ranges from military investigations to environment monitoring and ecological monitoring. The sensor networks generally comprises of several sensor nodes gathered from deployed environments in a large scale [1]. Sensor nodes in sensor networks face a major problem as sensor nodes are energy constrained and these have limited power, storage, communication, and processing capabilities. Thus the major problem in wireless sensor network is energy consumption. Thus to conserve energy and power sensor networks brings forth the concept of data aggregation [2]. This means

Natarajan Meghanathan et al. (Eds) : ACITY, VLSI, AIAA, CNDC - 2016
pp. 81–96, 2016. © CS & IT-CSCP 2016 DOI : 10.5121/csit.2016.60908

converting many values sensed from different environments into one single value and aggregated value is computed at sink by the use of some mathematical functions [3]. The technique for aggregation is used mainly for the reduction in amount of data to be sent in the sensor environments. As a result of reduction of amount of data communicated within WSNs, there is energy conservation of battery [4]. Sensor nodes send their readings to a special type of node for performing aggregation of data i.e., aggregators, that sends only the condensed or aggregated reading further [5]-[6]. These aggregators may be some kind of special nodes or normal sensor nodes also.

Sensor nodes requires high security as it prompts many security issues like confidentiality, data integrity, data authentication, key management, etc. High security is required in wireless sensor networks so it is one of the most popular research topics and much advancement have been reported on in recent years[7]. In this paper we mainly focus on security aspect of data transmission in WSNs and we propose a method of secure transmission of encrypted data across sensor nodes in sensing environments as well as secure key generation methods involved in attack detection and prevention in wireless sensor networks.

Encryption of data being transmitted in WSNs is necessary as this type of sensors can be subject to many different types of attacks. The attacker can either listen secretly the data being transmitted in WSNs (attacker may deduce the secret key) or send forged or duplicated data to sensor nodes, aggregators or base station (attacker may send forged data to cheat BS without knowing the secret key) or even compromise secrets of components of WSNs by capturing them. so as encryption is necessary sensor nodes must encrypt data on hop-by-hop basis. [8]-[9]-[10]-[11]. The mechanism of key generation involves an overhead activity making this an expensive and complicated operation [13]-[14]. Different key generation schemes have been proposed but they involve high computations for encryption of data and require more CPU, bandwidth and memory. For this reason we in this paper are using digital signatures along with two fish algorithm as a procedure for key generation[12].

2. DESIGN ISSUES AND ROUTING CHALLENGES IN WSN

Though the wireless sensor network have numerous applications, they have some restrictions like limited energy supply, low bandwidth of links connecting sensor nodes or limited computational power. The major goal of WSNs is to prolong the lifetime of the communication network and also prevent the problems in connectivity by implementation of aggressive and efficient energy management techniques. There are some challenging factors that influence the design of different routing protocols in WSNs. Here in the following we present an overview of some of the routing challenges as well as certain design issues that may affect the routing process in WSNs.

2.1. Node Deployment

This process of node deployment in WSNs is basically application dependent and it also affects the routing performance. There are two ways of Deploying Nodes, namely deterministic and randomized node deployment. The techniques in which sensors can be placed manually and data routing are done through predefined paths are called deterministic deployment. However in the case of random deployment the nodes are randomly scattered giving an impression of infrastructure of ad-hoc distribution. Optimal clustering becomes necessary if the overall distribution of nodes is non-uniform simply to allow energy efficient routing or to allow connectivity.

2.2. Energy Consumption

While performing computation or transmitting information's, the sensor nodes use their energy supply which is always limited in wireless environment. Thus the life of a sensor nodes shows a heavy dependence on the network battery lifetime. Every node in a multihop WSN plays dual role, both as a data sender and data router. Significant topological changes can be caused by power failures which may be a result of malfunctioning of certain sensor nodes. This may require the reorganization and rerouting of the packets being permitted in the network.

2.3. Node or Link Heterogeneity

Generally the sensor nodes are considered to be homogenous that is they all have some capacity in terms of communication, computation and power. But sometimes sensor nodes may have different capabilities or roles depending on their application as some of the applications may require a blend of sensors for monitoring pressure, temperature and humidity of the environment capturing the image or tracking of mobile objects. These special types of sensor nodes can either be independently deployed or all the different functionalities could be included in some sensor nodes. For example some hierarchical protocols can designate a cluster head to be different from normal sensor nodes. The cluster heads are chosen from among deployed sensors and are more powerful than the normal sensor nodes in terms of memory, energy and bandwidth. This handles the burden of transmission.

2.4. Fault Tolerance and Scalability

The failure of certain sensor nodes due to physical damage or lack of power or environment interface should not affect the overall performance of the sensor network. There may be a problem when many nodes may fail, the MAC and the routing protocols should accommodate the formation of new links or new routers to the data collecting BS. Thus multilevel redundancy id required in a fault tolerant sensor network. Scalability is another issue in WSN as the number of SN deployed in any sensing area they may be in the order of thousands or even more. The routing scheme used must be capable of working with the huge number of sensor nodes. Also the routing protocols being used must scalable enough to respond to any event or operation in the environment. Most of the sensors remain in sleep state until an event occurs.

2.5. Connectivity and Coverage

Higher node density in any sensor network prevent them from being isolated from each other. Thus the sensor nodes are expected to be well connected. This may not prevent different network topologies from being variable and also from the network Size shrinking due to failure of some sensor nodes. Thus the connectivity depends on the random distribution of sensor nodes. In WSNs all the sensor nodes obtain their own view of sensing environment. This view of sensor is limited both in accuracy as well as in range. Thus only a limited physical sensing area can be covered. Thus Area coverage also becomes an important design parameter in WSN.

3. PRELIMINARIES

3.1. Privacy Homomorphism Encryption

An encryption scheme with homomorphic property is privacy homomorphism encryption. The homomorphic property means that the algebraic operations on PT can be executed with the manipulation of the corresponding CT with the help of a key.

Dk (Ek (m1) O Ek (m2) = m1 @ m2,

Where Dk ( ) is decryption with key K., Ek ( ) is encryption with key K, O denote operations on cipher text and @ denote operations on plaintext.

PH schemes are of two types, similar to conventional encryption schemes. First one is Symmetric cryptosystems where keys are identical and second one is Asymmetric cryptosystem where keys are different. Symmetric PH schemes have greater efficiency as compared to Asymmetric PH schemes. The best known Asymmetric schemes are the one based on ECC (Elliptic Curve Cryptography) which provides the same security as RSA cryptosystem and that too with a smaller key size and cipher text. A 160-bit ECC cryptosystem provides the same security as provided by a 1,024-bit RSA cryptosystem [24].

3.2. Data Aggregation and Encryption

There is a major problem of aggregation of encrypted data in WSNs [23] which was firstly introduced by gira et al. in [10] and it was further refined in [15] .Homomorphic encryption schemes was used to enable arithmetic operations over cipher texts that is to be transmitted on a multi-hop basis. Secure aggregation also involves some problems with public-key encryption mechanisms [16]-17]. Solution to public key encryption mechanism is to equip nodes with private keys for increasing the security level. This limits the effect of attacker that compromises some of the nodes but this is not deployed yet because of certain reasons mainly being the high computational cost involved in encryption and decryption of plaintext and cipher texts. Also the expansion in bit size during plaintext to cipher text conversion involves high overhead hence depleting the sensors energy.

3.3. Routing Protocols

The efficiency of a sensor networks heavily depends on the routing protocols used. Energy Efficient & Secure Pattern Based Data Aggregation protocol (ESPDA) was proposed that considered data aggregation and security together for wireless sensor networks [18]. In ESPDA cluster heads prevent transmission of redundant data from sensor nodes making ESPDA as energy and bandwidth efficient. Next concept was Secure Reference Based Data Aggregation (SRDA) in which the raw sensed data by sensor nodes is compared with referenced data values and the only the differential data is transmitted rather than the raw data [19]. Hein Zelman, et al. [20] proposed a hierarchical clustering algorithm for sensor networks. This was Low Energy Adaptive Cluster Hierarchy (LEACH) based protocol. Here the operations were divided into rounds and during each round another set of nodes acts as CHs. Main advantage of this was that energy consumption is uniformly distributed among all the nodes and the main disadvantage was that it uses scheduling criteria based on (TDMA) time division multiple access which makes it inclined to long delays when it is applied to large sensor networks. An enhancement over LEACH protocol was published in [21]. This protocol was PEGASIS (Power Efficient Gathering in Sensor Information Systems). It was a chain based protocol designed for extending the lifetime of the network which elects a leader from the chain, based on residual energy level which results in average energy spent by each node being reduced. Virtual Grid Architecture (VGA) was another energy efficient routing paradigm proposed in [22]. This protocol used data aggregation and also in network processing to maximize the lifetime of the network as it performs data aggregation at two levels: local and global. PEGASIS greatly prolongs the lifetime of network when transmission range is limited and VGA saves more energy when transmission range is more.

3.4. CDA Based Privacy Homomorphism Schemes

Our work focusses on the solution for confidential data exchanges in WSNs that incorporates data aggregation. To the best of our knowledge, CDA (Concealed Data Aggregation) was the first concept that proposed a solution for end-to-end encryption along with the data aggregation model. In [8], the basic idea of CDA was introduced and it also showed the way to apply privacy homomorphism in WSNs. CDA provides end-to-end security along with providing in-network processing. They use algebraic properties of the applied PH: additive and multiplicative PH. In recent years, Castellucia, et al. Introduced an efficient data aggregation of encrypted data in WSNs and this is also based on additive homomorphism of encryption scheme [15]. Next concept introduced was CDAMA where the private keys is kept secret and it is only known by the base station. There is same public key for SNs in same group and no one outside knows the public key of the group. Also here BS extracts individual aggregated results from aggregated CT by performing individual decryption.

3.5. Digital Signatures

In some hostile environments, like a military battlefield, or environment monitoring, the broadcast authentication is an essential requirement to ensure the security and privacy of a Wireless Sensor Networks. The best way to provide broadcast authentication is to use digital signatures in sensor networks [25]. Public-key cryptography is considered to be too expensive for small sensor nodes, because it (like RSA) requires extensive computations and generally is not suitable for tiny sensors. In order to achieve Message integrity, Message Authentication Codes (MACs) are used. It allows for the application of digital Signatures that provide Data integrity and repudiation. Only the party that has the private key can create a particular signature. When a message along with a signature is received, only then the corresponding public key is used to verify the signature and once the signature verification is done, the receiver knows message integrity is still preserved. Digital signature is the most critical security services that cryptography offers. Digital Signature is an authentication mechanism which enables the sender to attach a unique code (signature). The signature is generated by taking the hash of the message and then encrypting the message with the sender's private key. It is an NIST standard that uses secure hash algorithm. The plaintext message, the message signature and the Public Key of sender are bundled together and transformed into signed and encrypted message using the Public Key of the receiver. The receiver unbundles received message and computes the message digest of the received message that is compared to the decrypted signature.

4. MODULE DESIGN

4.1. WSN set-up Model

In this module we set up a WSN environment in which network is divided into static clusters containing SN. Sensor nodes having limited energy and secure communication among them are necessary. Aggregator nodes are chosen based on residual energy level of nodes. Each sensor nodes sends the sensed data to corresponding aggregators which aggregates the received value and transfers the aggregated result to Base Station BS. We assume the Base Station to have immense computational power so it generates two types of keys, both public and private keys for sensor nodes using CDAMA scheme. All sensors have common public key but different private keys. Now the generated key is assigned to all the sensor nodes.

4.2. Aggregation Model

In WSN information is collected by sensor nodes from deployed environments and this collected information is forwarded to base station via multi-hop transmission based on cluster topology. This accumulated transmission results in high energy consumption for the intermediate nodes. Thus to increase the lifetime of the sensor networks cluster topology enables the intermediate nodes to perform data aggregation(AG).After performing aggregation AGs forwards the aggregated result to next hop. Aggregation of data takes place by two methods i.e., algebraic operations (e.g., adding or multiplying) or statistical operations (e.g., mean, median, mode, max, min). AG forwards only the aggregated result instead of forwarding the entire raw data.

4.3. Attack Model

Here in this model, we create two unauthorized sensor nodes called the attacker nodes which have more energy and threshold as compared to the normal nodes. There are different types of possible attacks on WSNs. Here we in this paper are considering the DOS attack Denial-of-Service attack which causes Black hole attack, Wormhole attack, Sybil attacks, Selective forwarding attacks etc. DOS attack is based on node-id. The attacker node behaves as normal nodes with its changed node id and receives data packets and drops them causing loss of data. Attacker nodes also change the threshold of the normal nodes thus drying the energy of the normal nodes. There are two methods followed by the attacker nodes here. Firstly, it traces the node id and changes the node id (based on node id) and secondly changes the threshold value (based on energy level).

4.4. Security Model

To ensure Data integrity and Data Confidentiality homomorphic encryption is used, which allows operations on encrypted data without decrypting them at the intermediate nodes thus preventing the access to plaintext. Considering the security issues in WSNs, we use Dynamic Intrusion Detection Protocol model (DYDOG) where Dynamic Intrusion Detection nodes are deployed which acts as both forwarding node and also intrusion monitoring and detection nodes with respect to data flow through sensor network. It uses secure session key management technique without deploying separate intrusion monitoring nodes. This technique makes network more dynamic and flexible against various kinds of attacks. Here in our work, we have used DYDOG technique along with a secure key generation scheme that is based on Digital Signatures and Two Fish Algorithms.

5. SYSTEM DESCRIPTION AND SECURITY OBJECTIVES

5.1. Network Architecture and Operating Mechanism

In this paper, we consider a wireless sensor network system consisting of a fixed base station and large number of sensor nodes. These sensor nodes are homogenous in functionalities as well as capabilities. We suppose, the sink as reliable always , but the sensor nodes are subject to be compromised by the attackers. In this wireless system, the data are sensed by the sensor nodes and are transmitted to a base station with the help of CHs that performs data aggregation. We also assume that, all sensor nodes and the BS use the symmetric radio channel, sensor nodes are distributed randomly, and are energy constrained. The protocol used is CDAMA that elects CHs, and a sensor node transmits the data to its CH.

5.2. Security Vulnerabilities and Objectives

Like all other type routing protocols in WSNs, CDAMA are vulnerable to number of security attacks e.g., jamming, spoofing, replay attacks, etc. Because of depending on the CHs for data aggregation and routing procedure, attacks involving CHs could be the serious to the network system. If an attacker compromises the secrets of a CH, it can provoke attacks such as sinkhole or selective forwarding attacks, thereby degrading the network performance. Also the attacker may intend to inject any forged sensing data into the network towards the CHs. If we use DYDOG and Digital Signatures along with the normal CDAMA protocol then we notice lesser attacks and improved network performance on the basis of throughput, packet delivery ratio, and throughput.

5.3. Protection from Vulnerabilities Mechanism

Wireless sensor networks are vulnerable to attacks like Denial Of Service (DOS) which includes mainly Black hole attack, Wormhole attack, Sybil attack, Jamming attacks and selective forwarding attacks. This is a serious problem in WSN. A packet drop attack or black hole attack is a type of DOS attack in which a node that is supposed to relay packets actually discards them instead. This occurs when a node is compromised by the attacker. Because the packets are dropped from a lossy network, it is very hard to detect and prevent these packet drops. The adversary can make several compromised nodes in Black hole intercepted region. Intruder can also sense or read the secret data from. Similarly wormhole attack records and also uses the secret data in unauthorized manner, Sybil attack causes faulty identification and the Selective forwarding attack data loss in wireless sensor networks. Against these various types of attacks Dydog model provides flexible and resilient solution by Dynamic Intrusion Detection Nodes for High-Data rate. Dynamic Intrusion Detection Protocol model (DYDOG) Design is based on data flow in Wireless Sensor Networks (WSNs). In this the Dynamic Intrusion Detection nodes are deployed which will act as forwarding node as well as an Intrusion Monitoring Node. The selection of dynamic intrusion detection nodes are from the neighbor’s non-forwarding node list using Secure Session Key Management approach without deploying any separate Intrusion Monitoring Nodes. Because of this the network becomes more dynamic and flexible against various types of attacks and provides availability of maximum monitoring node's with high error rate Wireless Networks.

Within the session itself depending on mobility the monitoring nodes dynamically change its behavior. For an attacker it creates problem to identify and attack these nodes within the limited session. By this technique the attacks and the Compromised nodes can be effectively and easily identified at runtime even in high data rate dynamic or static Wireless Sensor Networks (WSNs).

6. Our Scheme

We have used DYDOG mechanism for security enhancement of CDAMA. First we performed the Wormhole attack on CDAMA technique. Wormhole acts by three procedures.

1) Message duplication
2) Compromising the node-id of normal nodes
3) Packet dropping

To overcome this wormhole attack we use DYDOG mechanism, Digital signatures and Two fish algorithm.

Steps involved are as follows:

6.1. Key Generation Procedure

1. If source is transmitting data
2. Count the number of requests
3. Evaluate N [expr($len_q1)*($len_$q2)*($len_$q3)]
4. Initialize E
5. Randomize GEN as value of index.
6. Evaluate H = [(q1)*(q2)]*GEN
7. Evaluate Tmax = [(T)/(x)]
8. Evaluate P = [(q2)*(q3)*(GEN)]
9. Find Public key [((N)*(E)*(P)*(H)*(Tmax))]
10. Return Public key

6.2. Encryption Procedure

1. If data is received at destination
2. Count the number of reply
3. If request= message_id then randomize the value of R
4. Calculate cipher text as per expression C = [(M)*(P)+(R)*(H)]
5. Return the value of ciphertext as C.
6. Calculate aggregation count AGG_C=[(Message_id *P) + (Message_id *Q) + ($Message_id *H)]
7. Return the value of AGG_C

6.3. Aggregation Procedure

1. Compute the aggregated result as cipher text C'=C1+C2. It also includes the randomness of both groups.
2. Return C'

6.4. Decryption Procedure

1. Compute M,M = logp (q2q3*C)
2. Return M

6.5. DyDog Two Fish and Digital Signature Procedure

In this the Dynamic Intrusion Detection nodes are deployed which will act as forwarding node as well as an Intrusion Monitoring Node.

We define the following apps for using DyDOG along with Digital Signatures and Two Fish algorithm.

6.5.1. Cryptographic App

1. Initialize Crypto App with new app.
2. Use the catch variable in a procedure, if catch has crypto app and it should load the path of library where cryptography is available else it should return the error code.
3. Using the class namespace, eval , tcl drop , two fish and encryption is accessed. All will be accessed in the name space.
4. Variable of two fish version is specified i.e., version 0.1.
5. Package is provided for accessing the two fish and tcl drop and for calling the version initialized above
6. Package is provided for accessing the encryption and tcl drop
7. If the information is available for accessing the numversion of tcl return the same
8. Call the check module function for encryption
9. Define three procedures with keywords (Encrypt, Decrypt and Encrypt Password).

6.5.2. Cipher Text App

1. initialize cipher app with value new_app
2. if twofish.tcl file is available(file will be generated when running the code and disappears once executed) take it as source
3. check the packages required for Itcl, Tcl 8.4, tcltest,itwofish
4. proc h2b {hex}
   return [binary format H* $hex] //return the expression
5. proc b2h {bin}
   binary scan $bin H* dummy //scan binary value and make it as dummy value
   return $dummy //returning dummy value

6. If length of argument value is equal to 0 for each statement with digital signature number and cipher, then increment the testnum
7. Initialize the engine with two fish and digital signature number
8. Initialize encrypted value of engine in the encrypted block with the value of h2b and clear
9. Initialize the decrypted value of engine in the decrypted block with the value of encrypted which is obtained above.
10. if no string is encrypted using b2h or if no string is decrypted using b2h then reject the increment else approve the increment
11. Initialize a file in open status and trim the string and perform Monte Carlo test.
12. If the value of input vector and Monte Carlo value is equal create another engine using two fish and digital signature number.

6.5.3. Tests

We perform three tests here.

i. CBC mode test:

1. Initialize the engine with two fish and digital signature number.
2. Encrypt h2b (two fish object value) and pt (variable name) and make it encrypted with engine value.
3. Configure the engine with h2b (two fish object value).
4. Decrypt the encrypted value with engine and store it in decrypted app.
5. Access the itcl and delete the engine else call the value and check the below test

ii. Monte Carlo test

1. Initialize the engine with two fish and digital signature number.
2. Initialize the data with h2b (two fish object value) and pt (variable name).
3. Initialize the data with engine and encrypt block with data and make data encrypted.
4. Initialize the data with engine and decrypt block with data and make data decrypted.
5. Access the itcl and delete the engine else check the below test.

iii. ECB mode test

1. Initialize the engine with two fish and digital signature number.
2. Initialized encrypted value with engine and encrypted block with h2b (twofish object).
3. Initialized decrypted value with engine and decrypted block with called encrypted value.
4. Access the itcl and delete the engine.
5. If encrypted text does not match expectation or decrypted text does not match original plaintext then increment is failed otherwise approve the increment.
6. Initialize t with some message and encrypt the same with e and the decryption of block should be done while calling e.

6.5.4 Message App

1. Calling self to view the messages by node

2. Globally declaring ns with digital signature without encryption
3. Merge the messages viewed with respect to the message id's
4. Trace the node and node address
5. Calling self to send the size of message id and data with encrypt port.
6. Check the number of nodes and assign the node values to i.
7. Append the node id and message and assign Digital Signatures to all the nodes.

6.5.5 Check and Channel App

1. Check the value of packet size and if the expression of node boundary values is perfect with the data node,it will start transmiting the request otherwise node transmit stop
2. Assign each packet to channel and call the watch dog procedure and send it to all the channels.

6.5.6 Request

1. Creating new application called request.
2. Set flag as 0 and if source transmits data and reply from the destination is equal to source received reply then start the data transmission.
3. Else update the request and transmit the request till it reached the maximum value and initialize till request is maximum

6.5.7 Transmit

1. Create a new application called transmit
2. If source has the data received and the data received is equal to request, assign flag as 0
3. If flag is 0, drop the request, else transmit the request
4. If destinations have the received data and if node id request and node id reply are same then initialize the reply again

6.5.8 Reply

1. Create a new application called reply.
2. If reply is received and the received reply is not equal to source, assign flag as 1.
3. If flag is 0, transmit reply or acknowledgement or data and assign flag as 1 else drop the request.
4. Else assign flag as 1 and if reply received to node is not equal to source, transmit new reply or acknowledgement or data and assign flag as 1.

Count the values if node transmits are equal to 0 and if count is less than 2 then transmit count else stop the reply.

7. SIMULATION PARAMETER

This model is implemented using a network simulator 2.34. The simulation parameters are 500 X 500 sq. area, and consisted of 50 to 60 number of nodes with flat-grid topology, two ray ground ground radio propagation model and 802.15.4 MAC layer .AODV, CDAMA, AODV under Attack, CDAMA under attack and CDAMA along with DYDOG and Digital Signatures from different perspectives such as Average-delay, Packet Delivery ratio, Energy Spent and

Throughput. The network simulator set up is shown below in the table.

TABLE I SIMULATION PARAMETERS

SI. No.	PARAMETERS	Values
1	Simulation area	500 X 500 square meters
2	Propagation	Two ray ground propagation
3	Queue type	Drop tail
4	Antenna type	Omni antenna
5	Number of nodes	50 to 60 nodes
6	Topology	Flat grid topology
7	Routing protocol	CDAMA
8	Maximum packets in interface queue length	200
9	Network interface type	Phy/wireless
10	MAC type	802.11

8. SIMULATION RESULTS AND DISCUSSIONS

8.1. Average Delay

Average delay includes all the possible types of delays that may be either due to buffering during route discovery latency, or queuing at the interface queue or may be the transfer times of the data packets. The figure shows the end to end delay incurred in transferring the data from source node to sink node by different routing schemes. The maximum delay is in AODV with attack, Sybill attack followed by the CDAMA with attack. In an efficient network the average delay should be less and when CDAMA is compared to AODV under attack and CDAMA under attack, it has lesser delay but when we incorporate DYDOG along with Digital signatures the delay is further reduced.

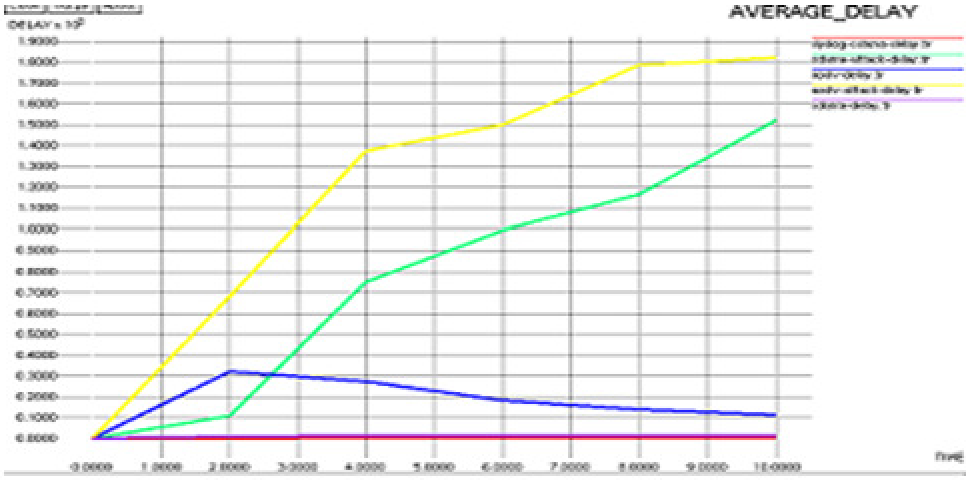

Fig.1. Variation of average delay with time

8.2. Packet Delivery Ratio

Packet Delivery Ratio is the ratio of the data packets that has been delivered to destinations to those that has been generated by constant bit rate (CBR) sources. The figure shows the packet delivery ration achieved by different routing techniques. The packet delivery ratio is highest for CDAMA enhanced technique followed by the normal CDAMA technique. In case of CDAMA under attack the number of packets sent is high but received number of packets is less so the PDR decreases for the AODV and CDAMA under attack.

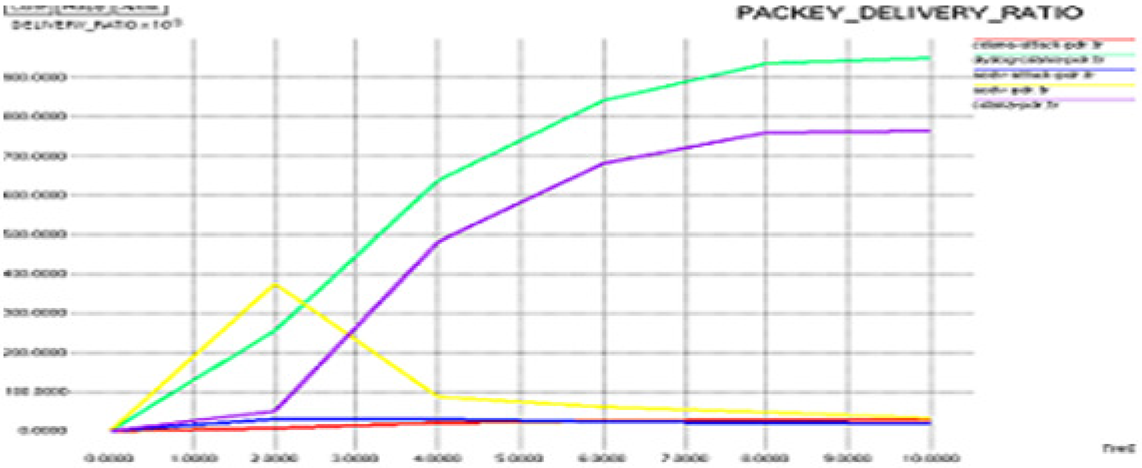

Fig.2. Variation of Packet delivery Ratio with Time

8.3. Energy Consumption

Average Energy Consumption by the sensor nodes in the network is one of the most important metrics to evaluate energy efficiency of the routing protocol that has been proposed. The figure shows the energy spent by nodes in the sensor network. Energy consumption for CDAMA technique is lesser than enhanced CDAMA because of some additional procedures like Two fish algorithms, Digital signatures and Dydog mechanisms. These extra procedures result in more energy consumption for enhanced cdama. Though DYDOG consumes little more energy but it also increases the throughput

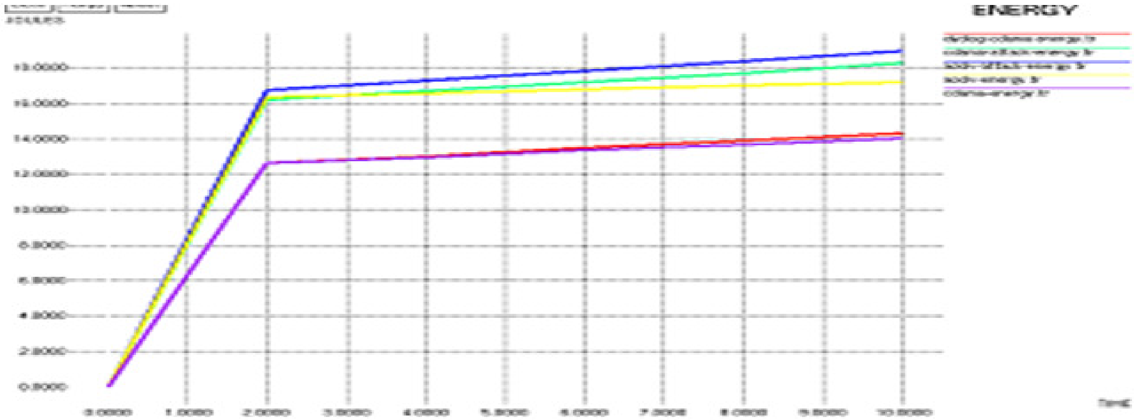

Fig.3. Variation of energy consumption with time

8.4. Throughput

Throughput is the total number of routing packets transmitted per data packets that has been delivered at destination. The throughput of CDAMA with DYDOG mechanism is more because of digital signatures along with Two fish algorithm. Though energy consumption is more but as throughput of overall transmission increases and hence the security also increases.

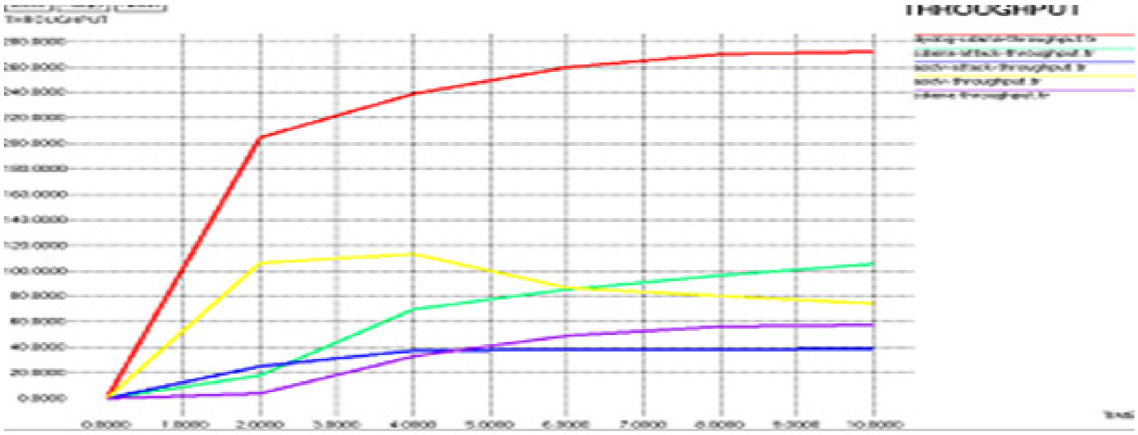

Fig.4. variation of Throughput with time.

9. CONCLUSION

The work proposes a secure, increased throughput and a better packet delivery ration scheme than normal CDAMA technique. Here the Dynamic Intrusion Detection Protocol (DYDOG) model is used along with Digital Signatures along with Two Fish Algorithms for CDAMA technique where cipher text of different applications can be aggregated together. While using these algorithms and protocols we have enhanced the working of CDAMA technique that mitigates the impact and reduces the overall damage to acceptable condition. CDAMA performs better than the traditional AODV routing protocol but the proposed technique provides higher security using Digital Signatures along with two Fish algorithm. The proposed technique defends the altered routing, selective forwarding and wormhole attacks. In this paper the energy consumption is still a issue as this technique leads to more energy consumption by the sensor nodes In our future work we will be proposing a technique for lesser energy consumption than the proposed technique.

ACKNOWLEDGEMENTS

The authors would like to thank everyone, just everyone!

REFERENCES

[1] I. Akyildiz,W. Su,Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks" IEEE Comm. Magazine, vol. 40, no. 8, pp. 102-114, Aug. 2002.

[2] R. Min,A. Chandrakasan, "Energy-Efficient Communication for Ad-Hoc Wireless Sensor Networks," Proc. Conference Record of the 35th Asilomar Conference Signals, Systems and Computers, vol. 1, 2001.

[3] B. Przydatek, D. Song,,A. Perrig, “SIA: Secure Informations Aggregation in Sensor Networks,” Proc. First International Conf. Embedded Network Sensor Systems, pp. 255-265, 2003.

[4] R.Chandramouli, S.Bapatla, and K.P.Subbalakshmi, ”Battery power-aware encryption.ACM transactions on information and system security,” pp. 162-180, 2006.

[5] K.Akkaya,M.Demirbas, RS.Aygun, “The Impact Of Data Aggregation on the performance of Wireless Sensor Networks,” wiley wireless Communication Mobile Computing (WCMC), J(8), 171-193, 2008.

[6] Alzaid,H, Foo,E, and Nieto J.G, “ Secure data aggregation in wireless sensor network-:a survey,” In the proceedings of the sixth Australasian conference on information security, Volume-81, pp.93-105, 2008.

[7] J.Girao, M. Schneider, and D.Westhoff, “CDA:Concealed Data Aggregation in wireless sensor networks,”Proceedings of the ACM workshop on Wireless Security, 2004.

[8] D. Westhoff, J. Girao, and M. Acharya, “Concealed Data Aggregation for Reverse Multicast Traffic in Sensor Networks: Encryption, Key Distribution, and Routing Adaptation,” IEEE Trans. Mobile Computing, vol. 5, no. 10, pp. 1417-1431, Oct. 2006.

[9] E. Mykletun, J. Girao, and D. Westhoff, “Public Key Based Crypto schemes for Data Concealment in Wireless Sensor Networks,” Proc. IEEE Int’l Conf. Comm. (ICC ’06), vol. 5, 2006.

[10] J. Girao, D. Westhoff, M. Schneider, N. Ltd, and G. Heidelberg, “CDA: Concealed Data Aggregation for Reverse Multicast Traffic in Wireless Sensor Networks,” Proc. IEEE Int’l Conf. Comm. (ICC ’05), vol. 5, 2005.

[11] J. Girao, D. Westhoff, E. Mykletun, and T. Araki, “Tinypeds:Tiny Persistent Encrypted Data Storage in Asynchronous Wireless Sensor Networks,”Ad Hoc Networks, vol. 5, no. 7, pp. 1073-1089, 2007.

[12] C.d. Westhoff,B.Lamparter, and A.Weimerskirch,“on digital signaturesin ad hoc networks,” J.Eur.Trans. telecom, vol.16, no. 5, pp. 411-425, 2005.

[13] R.Watro, D.Kong, S.Cuti, C.Gardiner, C.lynn, and P.kruus, “Sensor networks with public key technology”, in proc. 2nd ACM Workshop Security ad hoc sensor network, pp.59-64, 2004.

[14] C.karlof ,D.Wagner, ”Secure routing in wireless sensor networks: Attacks and countermeasures,”in the proc IEEE Int. Workshop Sensor Netw. Protocols Appl., May 2003, pp. 113-127, May 2003.

[15] C.castelluccia, E.Mykletun and G.Tsudik, “Efficient Aggregation of encrypted data in wireless sensor networks,” Mobile and Ubiquitous Systems: Networking and Services, 2005.

[16] E. Mykletun, J. Girao, and D. Westhoff, "Public Key Based Cryptoschemes for Data Concealment in Wireless Sensor Networks", IEEE Int'l Conf. Communications (ICC '06), pp. 2288-2295, 2006.

[17] T.ELGamal, “A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms,” CRYPTO,IT-31(4): pp. 469-472, 1985.

[18] H. Cam, S. O¨zdemir, P. Nair, D. Muthuavinashiappan, and H.O. Sanli, “Energy-Efficient Secure Pattern Based Data Aggregation for WSNs,” Computer Comm., vol. - 29, no. - 4, pp. 446-455, 2006.

[19] H. Sanli, S. Ozdemir, and H. Cam, “SRDA: Secure Reference based Data Aggregation Protocol for WSNs,” Proc. IEEE 60th Vehicular Technology Conf. (VTC ’04-fall), vol. 7, 2004.

[20] M. Younis,M.Youssef and K.Arisha,”Energy Aware Routing in Cluster Based Sensor Networks”, in the Proceedings of the 10th IEEE/ACM(MASCOTS2002), Fort Worth, TX , October 2002.

[21] S.Lindsay and C.Raghavendra, ”PEGASIS: Power Efficient gathering in Sensor Info. Systems”,international conference on communications, 2001.

[22] J.N.Al-Karaki,et al., “data Aggregation in Wireless Sensor Networks-Exact and approximate algorithms,” Proc IEEE Wks. High Perf. Switching and Routing 2004, phoenix, AZ , Apr.18-21,2004.

[23] Sanjeev Setia, a. Sankardas Roy and Sushil Jajodi “Secure Data Aggregation in Wireless Sensor Networks” Proc. of 33rd STOC, pp. 266–275, 2001.

[24] N. Koblitz, A. Menezes,S., Vanstone,“State of Elliptic Curve Cryptography,”Designs, Codes & Cryptography, vol. 19, no. 2, pp. 173-193, 2000.

[25] Cryptography and Network Security Principles and practices, William Stallings, Pearson Education, Fifth Edition.

AUTHORS

Bharat Bhushan (M’26).Date Of Birth-17th Dec 1989. Phd Scholar (Dept. of Computer Sc. & Engg.) student at Birla Institute of Technology, Ranchi, Jharkhand-835215, India.He has worked as Network Engineer for 1 years in HCL Infosystems Ltd., Noida

Keshav Kaushik (M’20). Date Of birth- 21/05/1996 BTech Computer Science & engineering student at HMR institute of technology & management.

.

Gadadhar Sahoo (M’60) Professor and Dean (Admissions and Academic Coordination) , Dept. Of Computer Science & Engg., Ph.D.., IIT Kharagpur. He has working experience of teaching field of 26 years and research experience of 31 years. He is now with Birla Institute Of Technology, Mesra, Ranchi.He has 167 publications in Natinal/International journals and 80 publications in National/International Conferences.Dr. Sahoo is also a member of ISTE.