International Journal of Advance Research in Engineering, Science & Technology(IJAREST),
ISSN(O):2393-9877, ISSN(P): 2394-2444,
Volume 2, Issue 8, August- 2015, Impact Factor: 2.125

Securing the Network using Asymmetric Key

Ambika.N

Dept. MCA(VTU), Dayananda Sagar college of Engineering, Bangalore

{ambika.nagaraj76}@gmail.com

Abstract: Sensor network is comprised of set of nodes deployed in the environment which needs to be monitored. These nodes play a vital role by monitoring unsupervised environment and sending the sensed data to the pre-defined location. These nodes press the panic button in case of emergencies. Hence these nodes can be deployed in any application ranging from simple to hazardous environment. These nodes are not tamper resistant and hence can't tackle the treats induced by the intruders in the network.

In this study, asymmetric key distribution management is being utilized to enforce better security in the network. The study combines the advantages of symmetric and asymmetric key distribution management. The paper increases the security measures by implementing better algorithm. The attacks addressed in this paper includes sinkhole attack, wormhole attack and Sybil attack are being tackled. The paper enhances security by providing backward and forward secrecy. In addition the study enforces authentication and integrity to the data in the network.

Keywords: Security, prevention and detection mechanism, asymmetric key distribution, malicious nodes, Authentication, Integrity, heterogeneous network

I. INTRODUCTION

Every technology whether small or large has its own benefits and threats. While embracing any kind of technology care needs to be taken to minimize the threats. Threats can be curtailed by focusing on its causes and trying to solve them by lessening its effect. One such technology is sensors which are being used widely in many applications [1-3] include military applications, habitat monitoring, environmental survey, forest fire surveillance and so on and so forth, the list goes on. These nodes being tiny, goes unnoticed. Viewing from this angle, these nodes can be deployed anywhere and anytime. These nodes are mainly deployed to monitor the environment, track the object of interest, and provide time-to-time data to the pre-defined location and many more.

These nodes are capable of organizing itself into a group and communicating to the pre-defined destination without any human intervention. These nodes are programmed in such a way that once they are deployed in any environment they initialize themselves, try communicating within their specified range, and have the ability to group themselves into a single unit, sense the environment, perform partial processing and communicate the same. Apart from these capabilities they are programmed to adopt simple algorithms to secure their conveyed packets to implement authentication and integrity. The intruder being very powerful communicating device adopts new mechanisms to purloin the packets in the midway before reaching its destination.

Two major types of attacks are obvious in these network, one being outside attack where the intruder will hear on the message/data being transmitted and other being inside attack where the intruder gains access of the keys and other information stored inside the nodes and the nodes behavior is being controlled by the intruder. The intruder after gaining access to the nodes, can induce false data into the network, can deny forwarding the data, and has the ability to manipulate them. Hence inside attack proves to be more precarious leading to breach in integrity and authenticity. This paper focuses on how to safeguard other nodes from the compromised nodes. To address such type of attacks, the nodes can be employed to adhere to some prevention techniques like key distribution and management. The nodes can fundamentally authenticate each other and then can utilize encryption keys to intensify its strength against different kinds of attacks. To increase the protection, detection mechanism [4-8, 9] can be employed which acquaint the network from the compromised nodes.

Two main kind of key distribution is being widely used in sensors. One being symmetric keys distribution and other asymmetric or public key distribution. Asymmetric key distribution [10] is being used in this paper. The study implements pre-distribution of keys followed by deployment of nodes in the required environment. Each node is identified by a unique key stored in it. This key along with the global time is utilized to encrypt the sensed data before transmission. The cluster head generates the encryption key by using its unique key and the global time. The key is being distributed to rest of the cluster members. The cluster head aggregates the data to all the cluster members. Group ID is being suffixed to the transmitted message to authenticate the source of the data. To add additional security forward secrecy is being implemented (since the time is a dynamic entity). Adding to this backward secrecy is being applied by deleting the previous encryption key utilized.

The intruder is being addressed as strong entity, adversary or terminal (considering laptop). One of the advantages using this kind of key distribution is , though the intruder gets hold on the key materials of any one of the

nodes in the network, the intruder will not be able to uncover the previous packet details (though the intruder has filched the data) as each key is unique on its own. In this paper, the cluster is addressed as group or unit.

The study is being segmented in the following manner. Section 2, summaries the related work previously published. Section 3 outlines the notations used in this paper. Section 4 provides a brief description of the assumptions made in the study. Section 5 elaborates the work by including the system architecture and different stages of entire process. Section 6 provides the analysis details of the study and a detailed proving of the study is being sectioned in segment 7 in form of simulation done using c#. The paper is concluded by briefing the contributions made.

1.1 Brief Contribution

- The base station/sink node is where the nodes in the network send their sensed and processed data.
- Heterogeneous network is being considered to monitor the environment and obtain relevant data.
- The nodes are randomly distributed in the environment.
- The status of the network regarding its anomalous activities is being monitored by multiple nodes at different points (detector and the cluster head) and any deviant activity is been intimated to other nodes in the network.
- Each node has a master ID, unique identifier ID, algorithms embedded before being deployed. The cluster is formed by exchanging by authenticating each other using master ID.
- The encryption key is generated for every session by the cluster head using its own unique ID and global time.
- The encryption key is also generated when the base station notifies malicious activity of the one of its cluster members.
- The detector also has a role to generate group ID (utilized to identify the group) using its location information and unique ID, which is latter affixed to the transmitted data (by the cluster head).
- The detectors in the cluster notify the abnormal activity of the nodes in that cluster.

II. RELATED WORK

Two types of key distribution are being used widely in sensor networks. Symmetric key distribution is one among them, where a random key is being chosen to encrypt the data. Asymmetric key distribution is another type of key distribution techniques. The advantage of this is much storage space is not required. But energy consumption is more since there would be exchange of information (to generate encryption keys) .The similar key distribution is done in [11], [12], [17], [24] and [25]. In general classical asymmetric method considers similar possibilities.

In [11] both RSA and elliptic curve cryptography are made possible using 8-bit CPUs with ECC, demonstrating a performance advantage over RSA. Another advantage is that ECC's 160 bit keys result in shorter messages during transmission compared the 1024 bit RSA keys. In particular the study demonstrates that the point multiplication operations in ECC are an order of magnitude faster than private-key operations within RSA.

In [12] the study shows that portions of the RSA cryptosystem can be successfully applied to actual wireless sensors using UC Berkeley MICA2 motes [19]. In particular, they implemented the public operations on the sensors themselves while off-loading the private operations to devices better suited for the larger computational tasks. The TinyPK system described in [12] is designed to allow authentication and key agreement between resource constrained sensors. The agreed upon keys may then be used in conjunction with the existing cryptosystem, TinySec [20]. To do this, they implement the Diffie-Hellman key exchange algorithm and perform the public-key operations on the Berkeley motes.

The Diffie-Hellman key exchange algorithm is being used in [17]. In this case, a point G is selected from an elliptic curve E, both of which are public. A random integer KA is selected, which will act as the private key. The public key is then $TA = KA * G$. Bob performs a similar set of operations to compute $TB = KB * G$. Alice and Bob can now easily compute the shared-secret using their own private keys and the public keys that have been exchanged. In this case, Alice computes $KA * TB = KA * KB * G$ while Bob computes $KB * TA = KB * KA * G$. Because $KA * TB = KB * TA$, Alice and Bob now share a secret key.

In [24], the authors propose a set of secure synchronization protocols for sender-receiver (pairwise), multihop sender-receiver (for use when the pair of nodes are not within single-hop range), and group synchronization.

[25] Compares three different public key algorithms securing wireless sensor networks to show that PKC can be used effectively in such environments. They are Rabin's Scheme, NtruEncrypt and NtruSign, and ECC (Elliptic Curve Cryptography). These algorithms are presented in the paper as proof-of-concept, showing that it might be possible to introduce PKC to sensor networks. The paper has focused on insider attack, namely, the false data injection attack. Public key cryptography alone cannot solve this problem, because node compromises in any event cause all cryptographic material to leak, including private keys. PKC is powerful for preventing outsider attacks, but suffers from the same weakness as symmetric methods.

In short, PKC localizes node compromise to the immediate neighborhood, because attacker gains only the compromised node's private key, but does not detect or prevent the false data injection attack in a foreseeable way. From resource consumption point of view, PKC requires a lot more power consumption, but scales well, because each node needs only the public keys of its neighbors to communicate. PKC can use to by two neighbor nodes to negotiate a secret key for symmetric encryption.

III. NOTATIONS USED

Table1: Depicts the notation used in the proposed model

NOTATION	MEANING
N_i	Cluster member of C_i cluster
C_j	i^{th} cluster of the network
CH_i	Cluster head of C_i cluster
T_i	i^{th} time chosen to generate the encryption key.
D_i	Detector of the C_i cluster
U_{ID}	Unique id stored in the cluster
E_i	Generated encryption key
T_p	The maximum length of the packet size of a node in the network
S	Total number of nodes in the network at the time of deployment
M_{ID}	Master key used to authenticate each other (nodes)
T_B	Time dispatched by the base station
T_T	Time Threshold set by the base station
G_{ID}	Group ID generated by the detector based on its location
T_D	Data Transmission time

IV. ASSUMPTIONS

4.1 The assumption of proposed model

The following assumptions are being considered.

- The base station is considered trustworthy. The base station generates unique ID for each node in the cluster and embeds the unique ID, master ID and necessary algorithms inside each node. The base station broadcast time to the network in every fixed interval of time along with the session time (encrypted using master ID).
- Any other node including cluster member, cluster head and detector are liable to be controlled by the intruder.
- The buffer size of all the nodes is fixed.
- The nodes are assumed to be uncompromised till they form the cluster.
- Each cluster contains a detector which monitors the activities of the cluster members and provides timely information to the base station. These detectors are assigned to monitor the activities of the cluster. The base station concludes the node to be compromised by comparing the data obtained by the detector and the transmitted data.
- The nodes deployed in the environment are liable to get compromised. The information stored in the nodes is revealed after the nodes are compromised. The intruder takes the control over the nodes, may impersonate itself as one of the nodes among the cluster, may tunnel the packets from one end to another and replay the packets.
- The detector has a GPS embedded inside it finds the location co-ordinates. It uses this data to generate group ID, for the cluster.
- The cluster head gives a comparison to the number of packets transmitted by the cluster member with the maximum count T_p.
- Cluster based routing is adopted.

4.2 The assumption of classical asymmetric model

The following assumption are made considering the previous work

- The data exchange between any two parties (private keys) should be done either by having a reliable node or the base station. To make data secure, the process has to be repeated frequently. This in turn increases energy consumption.
- If the public key is shared between the base station and node, each node's encryption key is going to differ from each other and hence the redundant data can't be eliminated by the cluster head (if cluster-based routing is considered).

4.3 The assumption of intruder model

The following assumptions are made

- The intruder is a strong entity capable of getting a hold of cost-effective nodes.
- The adversary is capable of introducing malicious packet inside the network, tunneling the packets to another location and replaying them, convincing (other nodes in the network) that it is one of the best nodes in the path to reach the pre-defined destination. This can be done by forging itself as one of the nodes destined to monitor the environment.
- The intruder either transmits packets beyond limits (to consume battery power of the network) or denies forwarding the packet.
- If not detected, the intruder can take the control of the entire network.

V. SYSTEM MODEL

5.1 System Architecture

5.1.1 Detector of the cluster

Waspmote with a microcontroller Atmel Atmega 1281, with transceiver ZigBee/802.15.4/DigiMesh/RF, 2.4 Ghz/868/900 MHz, program-data memory of 8K SRAM, external memory 128K FLASH ROM, 4K EEPROM, 2 GB SD Card is utilized. Waspmote integrates a GPS that can deliver accurate position and time information. Waspmote is either in sleeping or hibernating mode. Following the predefined interval programmed by the user, Waspmote wakes up, reads from the sensor, implements the wireless communication and goes back to the sleep mode. Each device is powered with rechargeable batteries and solar panel, making the system completely autonomous.

The main characteristic of Waspmote is its low power consumption. Table 2 illustrates the different modes and energy consumed. Waspmote, the mobile agent is capable to transmitting a signal up to 40km.

Table 2: Depicts the Energy consumption in Waspmote

MODE	ENERGY CONSUMPTION
ON mode	9 mA
SLEEP mode	62 µA
HIBERNATE Mode	0,7 µA

5.1.2 Other nodes of the cluster

The MICA2 mote is a third generation mote module used for enabling low-power wireless sensor network. It runs for more than a year with AA batteries. Mote Works is based on the open source TinyOS operating system and provides reliable, ad-hoc networking, over air-programming capabilities. It has 868/916 MHz multi-channel transceiver with extended range. It is based on ATMEGA 128L low-power microcontroller which runs Mote Works from its internal flash memory. It has 4K RAM program-data memory and 128K Flash external memory. It works in various modes. Table 3, illustrates different modes and energy consumed in MICA2 mote.

Table 3: Depicts the Energy consumption in MICA2 mote

MODE	ENERGY CONSUMPTION
Active mode	8 mA
SLEEP mode	< 15 µA
Transmit with maximum power	27 mA
Receive	10 mA

5.2 Embedding pre-deployment keys and Deployment of node in the network

The base station generates unique ID and embeds it inside each node from which the node is uniquely identified inside the network. The nodes are randomly deployed in the form of cluster. When the deployment is done, group of nodes are thrown from the plane consisting of Waspmote and MICA2 nodes. The nodes which are able to transmit/receive signals within the transmission range R are liable to fall into the cluster. The nodes broadcast HELLO_MSG message (equation 1), the nodes within the transmission range R acknowledges the transmission with ACK_MSG message (equation 2). The nodes further authenticate each other with master key M_{ID} (equation 3). The nodes which are able to communicate form the cluster.

$$N_I \rightarrow \text{HELLO\_MSG} \text{----------(1)}$$

$$N_J \rightarrow N_I\,(\text{ACK\_MSG}) \text{----------(2)}$$

$$N_I\,(M_{ID}) \leftrightarrow N_J(M_{ID}) \text{----------(3)}$$

5.3 Role of the detector

The detector being one of the cluster members is assigned a task to supervise the activities of all the cluster members in its group. The detector has to activate its GPS component and find its location. Using this as a parameter and its U_{ID} derives the group ID (equation 4). This is been passed on to the cluster head to attach at the end of the transmission message $T_{MSG.}$ The detector inside the cluster keeps a list of number of dispatched during session, dispatched time. The detector dispatches timely information using its unique ID (as encryption key) to the base station. This information is being utilized to check the integrity of transmitted data of the cluster. (Usually more than 1 detector is being enclosed within a cluster, hence if one detector is active other detectors behaves like a normal cluster member). In the equation 4, $LOC(D_i)$ finds the location of D_i.

$$\text{ENCRYPT\_GID}(U_{ID}, LOC(D_i)) \rightarrow D_i \text{ ----------(4)}$$

5.4 Choosing the cluster head and transmitting the data

The cluster head is chosen by the detector based on the reliability factor, its energy level and proximity from the base station. The detector generates ID to identify the cluster. This information is being dispatched to the base station and the cluster head (Equation 5). Let the time dispatched by the time base station T_B and time threshold is T_T, then T_i chosen by the cluster head is chosen using equation 6. The cluster head uses its unique ID and time T_i

to generate encryption key. This key is being distributed to all the members of the cluster.

$$BS \rightarrow ENCRYPT\ (T_B \parallel T_T) \text{ ---------- (5)}$$

$$T_i \rightarrow \int_{T_T}^{T_B} T\ dt \text{ ---------- (6)}$$

$$E_i \rightarrow GEN\_ENCRYPT\_KEY\ (U_{ID}, T_i) \text{ ---------- (7)}$$

$$T_{MSG} \rightarrow C_{i1} \parallel C_{i2} \parallel C_{i3} \parallel C_{i4} \parallel C_{i5} \parallel C_{i6} \parallel CH_i \parallel CH_j \parallel G_{ID} \parallel T_D \text{ ---------- (8)}$$

This encryption key E_i is generated for every session by the cluster head using its unique ID U_{ID} and chosen time T_i (equation 7). This key is distributed to the other cluster members. The encryption key is being utilized to encrypt the data before it is being transmitted to the cluster head. The base station eliminates the redundant data and then forwards the encrypted data T_{MSG} to the next hop/ base station(equation 8). In the equation 6, C_{i1}, C_{i2}, C_{i3}, C_{i4}, C_{i5} and C_{i6} are the encrypted data received by the cluster head from other cluster members of its unit. CH_i is the encrypted data of the cluster head suffixed to T_{MSG}. CH_j is the data received from cluster head of j^{th} cluster. G_{ID} is the group ID generated by the detector of the cluster and T_D is the time the data is transmitted to the next hop/base station.

6. SECURITY ANALYSIS

6.1 If a cluster member is assumed to be compromised

The intruder is a strong entity in the network much powerful than any sensor node. This entity is capable of confiscating the node and in turn getting hold of all the materials stored in that node. This malicious terminal can take the control of the node, introduce malicious packet in to the network (waste battery power), can impound the packets and replay them, and can tunnel to a different location and many in line.

The behavior of the cluster members is being analyzed by the detector and also the cluster head. Usually the nodes are being spread out in the network in such a way that at least 2-3 nodes can sense any activity simultaneously. Applying this concept, the cluster head has to obtain certain degree of redundant data. If it does not obtain redundant data, malicious activity is suspected among the cluster members.

The upper limit of transmitting data should not cross the threshold. Applying this concept the cluster member is given a maximum limit T_P. If the cluster member crosses this limit, the detector and the cluster head rings the alarm bell (signaling the base station). If the base station gets intimation beyond a certain threshold, the network is being informed about the malicious node's activity. The node is blacklisted in turn by the other nodes and seceded from the network.

6.2 If the Cluster head is assumed to be compromised

The detector inside the cluster keeps a watch on the cluster head. The detector generates a list consisting of number of packets delivered by the cluster members along with the transmission time and stores it in the table. This data is being transmitted to the base station. The cluster head aggregates the data transmitted by cluster members along with the transmission time. The base station makes a comparison between the data sent by the detector and the cluster head to check the reliability of data.

If the cluster head is compromised, it either broadcast too many messages or denies forwarding the data. Using this data, the behavior of the cluster head is analyzed (number of packets dispatched by the cluster members cannot exceed certain count). Another concept that can be considered is if the cluster count forwarding data varies with time, the time interval also varies. Hence the detector keep a count of how many clusters has forwarded the data.

If the detector finds the cluster head to be compromised, it sends the report to the base station. The detector for the moment instructs other cluster members to choose another cluster head to safeguard the cluster members from the suspicious cluster head. The detector generates the report and dispatches it to the base station. The base station after a certain threshold and cross-verification concludes the node to be malicious or not.

6.3 If the detector of the cluster is compromised:

The task of the detector in the cluster is to monitor other cluster members and sent timely report to the base station. The node in the cluster is assigned as a detector by the base station. At the time of deployment, one of the nodes is designated as a detector and deployed either manually by human/robot or randomly from the helicopter in the form of group. The detector is given authorization to control the some of the activities of the cluster. The former one being, to instruct the cluster members to opt another cluster head, if it suspects the cluster head to be compromised.

If the detector of the cluster is compromised, it either sends report randomly or very frequently. Other detectors of the cluster are instructed by the base station to monitor the suspicious detector. The detectors send their report to the base station based on which the base station concludes whether the base station is compromised or not.

If the base station concludes the detector D_i as compromised, the base station asks the other detector of the cluster to take the place of the previous one. The present nominated detector concludes its activity as a normal node and commences its task as a detector.

VI. SIMULATED RESULTS

The paper is simulated using C#. 520 nodes are deployed in the area of 500m * 500m. Among 520, 70 nodes are Waspmote and other 450 nodes are MICA2 nodes. The Waspmote is basically deployed to televise its position (in terms of location), generate group ID using location information and dispatched to other cluster members. Each cluster contains 7-8 cluster members. The unique ID stored in the node is of 122 bits in length. The encryption key length is of 132 bits in length. In the table the maximum value is 1, which is considered as 100%.

Table 4: simulated results

DESCRIPTION	QUANTITY
Dimension of the network	500m * 500 m
Distribution of nodes	Uniform
Number of cluster members in each cluster	7-8
Number of clusters having 7 cluster members(including detector)	40
Number of clusters having 8 cluster members	30
Total number of clusters	70
Total number of nodes in the network	(8*30)+(7*40)= 520
Length of Unique ID	122 bits
Total length of encryption key	132 bits
Threshold time	0.1 nanoseconds
Number of detectors in the cluster	2 -3

7.1 Energy consumed

Energy consumption becomes one of the prior aspects in wireless sensor network as these nodes run on battery. These sensor nodes are deployed in unattended environment hence the battery can't be recharged.

Figure 1: Energy consumption (without any attacks)

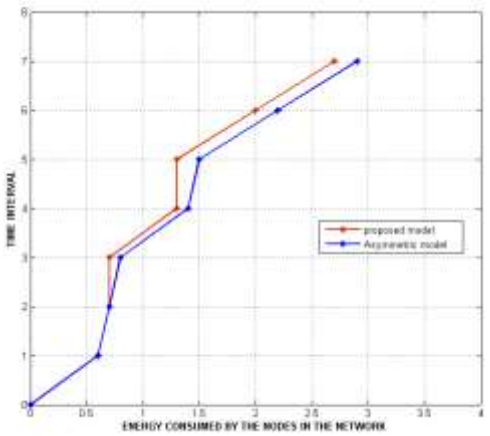
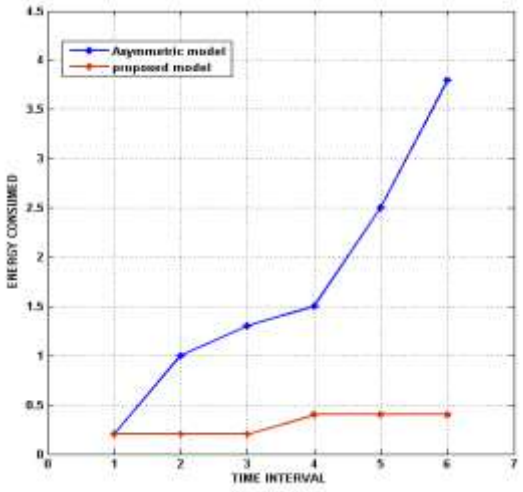


Figure 2: Energy consumption (under attack)



In this paper, Asymmetric key distribution is being utilized. Utilizing this method also improves security to larger extent, because as the cluster head generates dynamic encryption keys to encrypt the data. If one of the nodes is compromised, other nodes data go unaffected.

Compared to the classic asymmetric key distribution technique where the same key is utilized for every session, the proposed work uses time parameter (dynamic entity) which assists the cluster head to change the encryption key for every session. Another advantage is if any of the data acquired by the intruder, the intruder will not be able to launch any kind of attack (wormhole attack) or will not be able to interpret the data.

Comparing the proposed work to the classic asymmetric key distribution method (does not have pre-embedded key, rather the keys are dynamically distributed) the proposed model consumes 0.2% more energy (considering both the models are not under any attack). Fig 1, provides a comparison between classic asymmetric key distribution and proposed work. As the detector is deployed in every cluster and multiple clusters summate their effort to confiscate other nodes getting compromised. The detector will have the authority to instruct the members of the cluster

to change the cluster head, if the detector finds the cluster head as malicious.

If the cluster head is compromised, either the packets delivered by the cluster members may not be forwarded to the base station or the cluster head may repeat transmitting the packet again and again. The clusters which forward this data will waste energy of other nodes in the network.

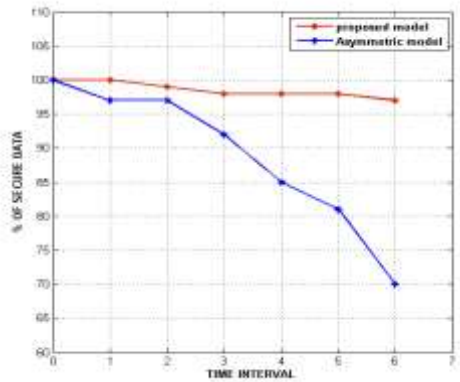
If the cluster member is compromised, it frequently sends data to the cluster head which wastes energy of the cluster head and the nodes through which the packets travel to reach the base station. The proposed work utilizes detector which will be able to monitor such activities and take control over the situation. Simulating the work, classic Asymmetric model consumes 3.4% more energy than the proposed model. The proposed model consumes 3.2% less energy than Asymmetric model in totally. Fig 2, gives a comparison of the energy utilized by the classic asymmetric model and proposed work.

7.2 Sinkhole attack

This is one of the attacks [21-23] encountered when the data is transmitted from one end to another. The nodes under this attack publicize as a node closer to the base station. Other nodes unknowingly choose this compromised node to forward the data. By doing this the compromised node can either replay the forwarded data and devastate the energy of other nodes in the path followed by them to reach the base station.

In the proposed model, the detector in the cluster keeps a watch on the activities of the nodes in the network. If any of the cluster members including the cluster head transmits packets beyond a certain limit, the detector in the cluster portrays its activity and reports the activity to the base station. The base station evaluates the activity and concludes to exclude the node from the cluster if the member is confirmed as a compromised node. As the nodes are being watched, the network is remains secure from Sinkhole attack.

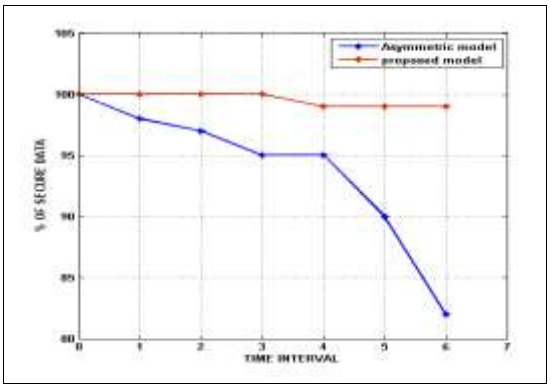
Figure 3: Effect of sinkhole attack



Without a detector, the activities of the cluster cannot be monitored and the abnormal activity cannot be traced. Utilizing the proposed model, 27% of data can be made secure. Fig 3, portrays how Sinkhole attack is being minimized compared to the classic asymmetric model.

7.3 Sybil attack

Figure 4: Effect of Sybil attack

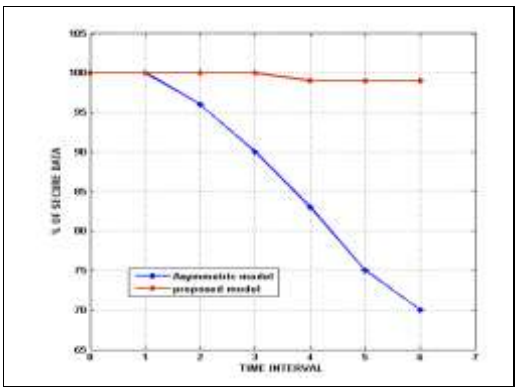


This is an attack [13-14] launched by the adversary, where the adversaries impersonate as a node duplicating the unique ID of one of the nodes in the cluster and misleading the cluster members.

The data will not be disclosed to the intruder as the time changes continuously (time is a variant) enabling forward secrecy. After the data is encrypted and dispatched, the encryption key is deleted (provides backward secrecy). Hence though, the nodes are imposed by the adversary, the data dispatched cannot be interpreted (if the adversary is able to take a hold on the data). Compared to symmetric key distribution schemes where the key is randomly chosen, the proposed work changes its encryption key for every session. Implementing the proposed work in the form of graph (figure 4), 17% of the data is secured compared to Asymmetric key distribution (without detector facility).

7.4 Wormhole attack

Figure 5: Effect of wormhole attack



Wormhole attack [15-16] is a kind of attack where the intruder embezzles the packet from reaching the next hop

(reliable one) but rather ducts the packet to different location and retransmits it to the base station/next hop from that location. Performing this activity provides a false illusion to the base station (about the environment). The base station may not be able to take accurate decision.

The keys are unique to each node at different instances of time and hence the base station will have an accurate idea which node can utilize which key at an instant of time. As the keys keep on varying for every session, the base station will have an idea of which node has utilized the key. Adding to this group ID also authenticates the cluster. Apart from this, detectors are deployed (reliable) in all the clusters to keep an eye on the cluster members. The detector can entrap this misbehavior and can detach the node (suspicious) from the cluster. If the node is confirmed to be a malicious node, the node is completely and permanently detached from the network (based on the decision of the detectors and base station). From the graph (fig 5), 29% of data is made secure by utilizing the proposed model when compared to classical Asymmetric model.

Table 5: Data obtained during simulation

PROBABILITY	PROPOSED MODEL
Probability of detection of compromised nodes	>=0.97
Probability of false alarm	<=0.03
Probability of data integrity	>=0.98
Probability of reliable data reaching base station	>=0.92
Threshold	The changes in the position of cluster head is made at the first instance, hence the threshold is taken as 1%

Table 5 portrays the simulation results. The simulation is been focused to eliminate the compromised node in the network. The proposed model detects compromised node in time with the probability of 0.97 or greater. The intruder can send false alarm to the base station. The probability of false alarm is lesser or equal to 0.03. From the simulation result, the proposed model is assuring probability of 0.92 or greater reliability of data. The base station needs to decide whether the node is malicious or not when it receives report from the detector or the cluster head. Doing cross-verification, the base station assumes a threshold of 1% to warn other nodes in the network.

VII. CONCLUSION

The paper utilizes asymmetric key distribution method to generate encryption key. The key is generated by using global time as one of its parameter. The paper applies group-oriented transmission of data. The key is changed for every session and hence the data is secured from different kinds of attacks. The effect Sinkhole attack, wormhole attack and Sybil attack are being reduced to a larger extent using this work. The study employs backward and forward secrecy. In addition authentication and integrity is being enhanced with limited energy consumption compared to classical asymmetric key distribution.

REFERENCES

[1] G.J. Pottie , W.J. Kaiser (2000) Wireless Integrated Network Sensors. Comm. ACM, vol. 43, issue 5, pp. 51-58.
[2] C. Chong , S. Kumar (2003) Sensor Networks: Evolution, Opportunities, and Challenges. Proc. IEEE, vol. 91, no. 8, pp. 1247-1256.
[3] I. Akyildiz, W. SU, Y. Sankarasubramaniam, E. Cayirci (2002) A Survey on Sensor Networks. IEEE Comm. Magazine, vol. 40, no. 8, pp. 102-114.
[4] S. Kumar , E.H. Spafford (1995) A Software Architecture to Support Misuse Intrusion Detection. Proc. 18th Nat'l Information Security Conf.
[5] K. Ilgun, R.A. Kemmerer, P.A. Porras (1995) State Transition Analysis: A Rule-Based Intrusion Detection Approach. IEEE Trans. Software Eng., vol. 21, no. 3, pp. 181-199.
[6] T. Bass (2000) Intrusion Detection Systems and Multisensor Data Fusion. Comm. ACM.
[7] Y. Zhang, W. Lee (2000) Intrusion Detection in Wireless Ad Hoc Networks. Proc. IEEE/ACM MobiCom.
[8] R. Zhang, D. Qian, C. Ba, W. Wu, X. Guo (2001) Multi-Agent Based Intrusion Detection Architecture. Proc. Int'l Conf. Computer Networks and Mobile Computing.
[9]] Oleg Kachirski, Ratan Guha (2002) Intrusion Detection using mobile agents in Wireless Ad Hoc Networks. IEEE Workshop on knowledge Media Networking (KMN '02), pp.153.
[10] R. C. Merkle. Protocols for public key cryptosystems. In Proceedings of the IEEE Symposium on Research in Security and Privacy, April 1980.
[11] N. Gura, A. Patel, A. Wander, H. Eberle, and S. Shantz. Comparing elliptic curve cryptography and rsa on 8-bit cpus. In In 2004 workshop on Cryptographic Hardware and Embedded Systems, August 2004.
[12] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus. Tinypk: securing sensor networks with public key technology. In Proceedings of the 2nd ACM workshop on Security of Ad hoc and Sensor Networks (SASN '04), pages 59–64, New York, NY, USA, 2004. ACM Press.
[13] Kuo-feng Ssu, Wei-tong Wang, Wen-chung chang (2009) Detecting Sybil attacks in Wireless Sensor Networks using neighboring information. The International Journal of Computer and Telecommunications Networking , Volume 53 Issue 18 .doi>10.1016/j.comnet.2009.07.013
[14] Ren xiu-li,; Yang Wei (2009) Method of Detecting the Sybil Attack Based on Ranging in Wireless Sensor Network. 5th International Conference on Wireless Communications, Networking and Mobile Computing, pg- 1-4, doi>10.1109/WICOM.2009.5302573
[15] Zhibin Zhao, Bo Wei, Xiaomei Dong, Lan Yao , Fuxiang Gao (2010) Detecting Wormhole Attacks in Wireless Sensor Networks with Statistical Analysis.

International Conference on Information Engineering (ICIE), pg: 251-254, doi> : 10.1109/ICIE.2010.66.
[16] Honglong Chen, Wei Lou, Xice Sun, Zhi Wang (2010) A secure localization approach against wormhole attacks using distance consistency. Journal EURASIP Journal on Wireless Communications and Networking - Special issue on wireless network algorithms, systems, and applications, doi>10.1155/2010/627039.
[17] D. J. Malan, M. Welsh, and M. D. Smith. A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography. In First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON, 2004.
[18] G. Gaubatz, J.P. Kaps, and B. Sunar. Public key cryptography in sensor networks - revisited. In 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004), 2004.
[19] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. E. Culler, and K. Pister. System architecture directions for networked sensors. In Architectural Support for Programming Languages and Operating Systems, pages 93–104, 2000.
[20] C. Karlof, N. Sastry, and D. Wagner. Tinysec: A link layer security architecture for wireless sensor networks. In Second ACM Conference on Embedded Networked Sensor Systems (SensSys 2004), pages 162–175, November 2004.
[21] Sharmila. S, Umamaheswari.G. (2011) Detection of Sinkhole Attack in Wireless Sensor Networks Using Message Digest Algorithms. International Conference on Process Automation, Control and Computing (PACC),pg : 1-6;doi>10.1109/PACC.2011.5978973
[22] Krontiris. I, Giannetsos. T, Dimitriou. T. (2008) Launching a Sinkhole Attack in Wireless Sensor Networks; The Intruder Side. IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, pg : 526-531, doi > 10.1109/WiMob.2008.83
[23] Edith. C. H. Ngai, Jianchuan Liu, Michael. R. Lyu (2007) An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks. Journal Computer Communications ,Volume 30, Issue 11-12; doi>10.1016/j.comcom.2007.04.025.
[24] S. Ganeriwal, S. Capkun, C.-C. Han, and M. B. Srivastava. Secure time synchronization service for sensor networks. In WiSe '05: Proceedings of the 4th ACM workshop on Wireless security, pages 97–106, New York, NY, USA, 2005.
[25] G. Gaubatz, J. P. Kaps, E. Ozturk, and B. Sunar, "State of the art in ultra-low power public key cryptography for wireless sensor networks", Third IEEE International Conference on Pervasive Computing and Communications Workshops, pages 146–150, 2005.