© 2016 IJSRSET | Volume 2 | Issue 4 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

An Optimal Approach to Select Watchdogs using Secure Key management Schemes in Clustered Wireless Sensor Networks

S. Rajasoundaran, P. Narayanasamy, S. Kasirajan

Anna University, Chennai, Tamil Nadu India

ABSTRACT

Wireless Sensor Networks (WSNs) are widely used in different types of applications. Due to the open medium of these networks, they are vulnerable against the intrusions or attacks. Any adversary can have the opportunity to insert their attacks to dump the performance of the sensor nodes or the overall network. To identify the adversaries, Watchdog nodes are selected based on different mechanisms with limited assumptions. Once the adversary has the internal network knowledge, then the conventional monitoring mechanisms could be useless. This work provides resilient solution over these critical issues by selecting the watchdog nodes using On-Demand Dynamic Monitoring and Routing Protocol (ODDMRP) with secret key management techniques. Here, the watchdog node selection processes and the monitoring processes are kept secret against any type of adversary or against various attacks.

Keywords: Wireless Sensor Networks, Attacks, Watchdog Nodes, Key Generation, ODDMRP.

I. INTRODUCTION

Wireless sensor networks is the latest research topic due to its importance and need for mobility and low power consumption solution in many of the real world challenges. Their applications include Military applications, Human centric applications, Support for logistics, Environmental monitoring, Applications to robotics [10]. In these applications a huge number of hazards can occur which can range from high temperatures, fragile surfaces, noisy electrical affects and even explosive gases. In such hazardous conditions, controlling and monitoring of communication traffic and sensor nodes becomes tedious. Also there is always security breach in wireless sensor networks if it is in the case of ad-hoc nature and inability to perform direct operations. The attacks may include Denial of Service that can range from simply jamming the sensor's communication channel to more sophisticated attacks designed to violate the 802.11 MAC protocols [11] or any other layer of the wireless sensor network. It also encompass a variety of techniques including node takeovers, attacks on the routing protocols, and attacks on a node's physical security.

To detect various types of anomalies over wireless medium is very difficult without monitoring. In order to defend these type of anomalies various types of cryptographic method pertaining to wireless networks are used, but these are only first line of defence which the attacker could easily get pass through. On the other hand, multi-path clustering is also necessary for effective data processing in Wireless medium. Hence as a solution to the above problem, hierarchical Wireless Sensor Networks (WSNs) are scenario is used in this work. The election of cluster head in cluster based WSN must be effective and to improve the life span of the entire network, energy efficiency is always a key design issue in the WSN. Hence to address these issues, Secure Low-Energy Adaptive Clustering Hierarchy (SLEACH) is used.

In this work, the clustered network is formed using the [9] SLEACH protocol. SLEACH is a secure cluster head election protocol which elects the cluster heads based on low energy level and the identity verification. To provide secure channel for data transfer, a Pre-key distribution scheme is used. Traditional key management schemes include probabilistic and deterministic schemes. Both the schemes have some disadvantages. Hence Randomized Combinatorial Design (RCD) based pre key distribution is used. The key distribution is done in two phases. They are RCD for initial key distribution and Random Markov Chain Model (RMCM) where the next state depends only on the current state and not on the events that preceded it. This is used to create different sample values from location coordinates of the moving nodes by incorporating RCD keys. A session is created for communication between two

nodes use Canetti Krawczyk Proof Model (CKM) in order to provide secure multipath creation for routing.

The basic methodology of this work is that the nodes are created and the nodes are formed into clusters. From these clusters the cluster head is elected using SLEACH to verify whether the elected cluster head is legitimate or not. If an attacker with Denial of Service attack tries to attack the system, then there is a possibility that some nodes being internally attacked. These nodes are known as compromised nodes. These nodes are being detected and then prevented using [7] KDD data set. Key distribution is done using RCD and RMCM. A session is established before the nodes communicate with each other using [12] CKM. By this authentication, security is provided for the messages that are passed between the nodes. The Triple key method is mainly used for inter-cluster communication in which a node from one cluster communicates with the node in the other cluster.

The most important and fundamental objective when compared to the existing systems is that the election of cluster head takes place in the most secured way and besides that the energy consumption during this process is also less. The algorithm used is known as the SLEACH in which the digital signature of RSADS / DSA is used. Before a node is being elected as a cluster head its legitimacy is checked with the digital signature which has been placed in the Base Station. The node once chosen as the cluster head will not be elected as the cluster head again in order to reduce the energy consumption. The node with the least threshold value is elected as the cluster head.

The node when being attacked by an external attacker are detected and prevented. Compromised nodes are nothing but they are attacked internally by an external attacker. In order to get rid of this, the KDD data set is used to detect and prevent the compromised nodes behaviour. The communication between nodes takes place in the most secured way by providing different methods to generate keys which cannot detected by the external attackers. The same pair wise key generation method is used every time but with different inputs for different phases. This helps to provide a network system with less energy consumption. Multiple session communication can take place with the use of CKM where one node can communicate with one or more nodes simultaneously.

It has been observed that security in wireless sensor networks is an important issue and the work contributes a lot to the solution. The election of cluster head is taking place through the SLEACH algorithm in order to elect the legitimate node as the cluster head. Communication between nodes is taken with the help of RCD which uses hashing function which is very difficult to be intruded by the attacker. In RMCM , the position of the node is used as the parameter to develop the key for communication, since the node is always in mobility it is difficult to detect the key as the node keeps on changing its position. Triple key method is used for inter-cluster communication in which only one key has to be generated for two sessions which are created during inter-cluster communication.

II. METHODS AND MATERIAL

2. Related Works

In this section some of the existing cluster based intrusion detection schemes and also some of the existing key distribution schemes are discussed. With these already existing proposals in mind the work has been done.

Sushmita Ruj et al [1] and Kasirajan et al [2] proposed the schemes for pre key distribution. The authors used combinatorial design as base for their proposed scheme. A pair wise key distribution scheme and a triple key distribution scheme were build based on the combinatorial design theory. Their scheme has advantage over other schemes already been proposed in terms of security and bandwidth requirements. Polynomial-based scheme is applied so that every three nodes have a common key. This scheme is c-secure, where c is degree of polynomials used. The open problem stated is to design a secured routing algorithm based on the triple key to preserve anonymity at the same time guaranteeing full security. Sooyeon Shin et al [4] proposed an intrusion detection protocol based two-level clustering for WISN. Since one hop clustering are not practically suited for data gathering and energy efficient, they proposed a hierarchical framework based on two-level clustering which consists of the first clustering (multi-hop clustering) for efficient data gathering and the second clustering (single hop clustering) for effective intrusion detection. There is an open problem in the proposed framework in regard to the heterogeneous WISNs.

Tingyao Jiang et al [5] proposed new scheme which uses a clustering algorithm to build normal traffic behaviour to detect abnormal traffic patterns. The cluster-based wireless sensor network comprises of clusters and a sink node. After running intrusion detection algorithm the sink node detects suspicious traffic and reports the cluster about where the suspicious traffic is from. Then it broadcasts the

messages to the cluster members to adjust the detection parameters. After adjusting the parameters, the cluster members are using the new parameters to detect. If the detection is still fail, the sink node continues to inform the cluster to adjust until the cluster members can detect suspicious traffic.

In the proposed method the clustered head sometimes may be an attacker or compromised node, this is overcome by the SLEACH (Secure SLEACH) algorithm in which the node's legitimacy is checked through the digital signature (RSADS/DSA) which is available in the base station. In the work there is a multipath communication, so that when a session has been established from one node to the other there can be no other communications with the other node until the previous session closes, whereas in the work multi-path communication have been done so that multiple sessions can be created with a particular node. For each session separate keys have to generated, in order to avoid this RMCM has been used in which the node's position as the current state from this the keys can be generated for the upcoming stages. This helps in reducing the energy consumption. This also provides a very high security to the network through which communication takes place.

3. System Architecture

The ideal network is the wireless sensor nodes in mobility. The Base Station does the computational part as there is resource constrains involved in the sensor nodes. The Base Station has the digital signature (RSADS/DSA) of all nodes of the network and the KDD data set which is discussed later. The clustered network is formed using SLEACH (Low-Energy Adaptive Clustering Hierarchy) protocol. The cluster head is chosen by using a stochastic technique. Nodes that have become a cluster head cannot become cluster head again for *I* rounds (i.e.) each node have the probability of 1/I of becoming cluster head in each round. The tasks of SLEACH are falling under two phases, one is setup phase and another one is steady phase. In setup phase, the cluster head is elected using signature verification techniques and the energy considerations. In steady phase, different key management approaches (RCD, RMCM and CKM) are used to make multiple layers of authentication verifications to make the cluster head more valid. To select first level cluster heads, the equation follows,

L=DSA/RSADS [I/(1-I*[r mod (1/I)])] if n Ɛ G ---------- (1)

where**,** L - Threshold value, I - The needed percentage, r- Number of rounds, n -Random number between 0 and 1, G - Set of nodes not selected as cluster head in last 1/I rounds . The Cluster head election algorithm follows

Step 1. Calculate the random percentage P using random function.
Step 2. r is the number of rounds that will be iterated till the cluster head is elected.
Step 3. The threshold t is calculated by the above formula
Step 4. Then choose a random number between 0 and 1
Step 5. The random number chosen should be less than the threshold t if so then that node will be elected as cluster head
Step 6. In addition to step 5 the digital signature of the node is verified with the base station and if it pass then the node is elected as cluster head.
Step 7. Redo the steps

After a node is self-selected as a cluster head, it advertises this to all its neighbours. The sensor nodes receive advertisements and they determine the cluster that they want to belong to, based on the signal strength of the advertisements from the cluster heads. The sensor nodes inform their cluster head that they are the members of the cluster, and then the cluster head assigns a time slot for every sensor node in which they can send data to the cluster head.

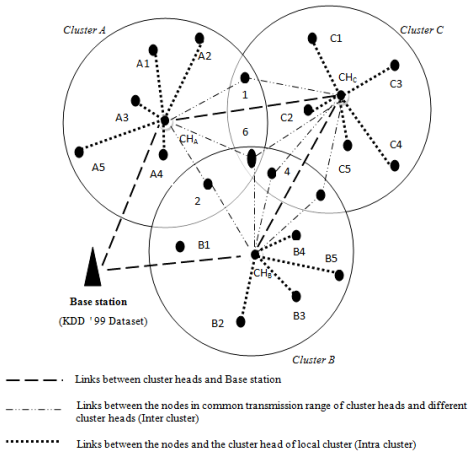


Figure 3.1 – Cluster Formation

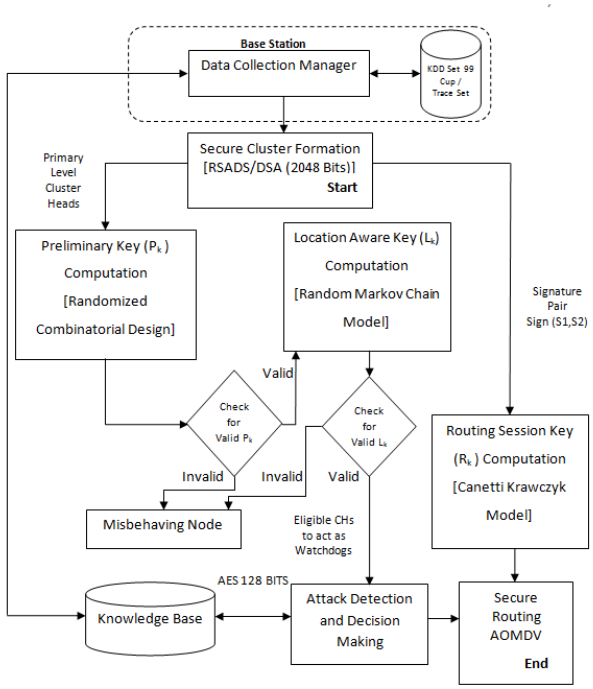


Figure 3.2 – Secure key management based watchdog selection scheme

The above figure illustrates the three tier key management based watchdog selection scheme and upcoming sections describes the techniques used to select the watchdogs in secure way.

3.1.1 Randomized Combinatorial Design (RCD)

The working principle of RCD is given below

Step 1. The key P_k for each node is computed in the base station to reduce computational overhead.
Step 2. For each node 3 values (l, m, n) are generated which is actually the subset of X
Step 3. These l, m and n values act as an identifier to generate pair base key for Primary level cluster heads (PLCHs)
Step 4. The set of keys P_k(s) for PLCHs of the network are distributed through authorized nodes.
Step 5. The key for each PLCH is given to RMCM.

3.1.2 Random Markov Chain Model (RMCM)

The second approach is the Random Markov chain model in which the position of the node is used to generate the key using the pair wise approach. Since the position of the node keeps on changing it is very difficult to detect the key.

Step 1. Find the location tuple (i , j , u) from geographical coordinates
Step 2. Compute $L_k=M_{i,\ j,\ u}(l, m, n)$; L_k- Location aware random key
Step 3. Check the validity of L_k
Step 4. Identify eligible cluster heads to act as watchdog

The key is generated using the same algorithm mentioned above.

In this system, the parameter for the current state used is the **position** of the node. By keeping the position of a particular node as the parameter the key is created using pair wise key generation method. Since the position of the node keeps on changing it is very difficult for the attacker to identify the key. There are two types of communication systems proposed in the system they are inter-cluster communication and intra-cluster communication. In intra-cluster communication the communication takes place between two nodes which are in the same cluster, the key that is generated is (SHA-1) hashed value of the identifier of the each of the node. The other type of communication is the inter-cluster communication in which the node in one cluster communicates with the node in the other cluster. The communication takes place in the following manner, first the node in one cluster creates a session with the cluster head of the other cluster, and then the cluster head creates another session with the designated node. In these situation two keys has to be generated for each session, to avoid these problem Triple Key Method is used for key generation in inter cluster communication. In which the same key is used by the 3 nodes in communication. The key is generated by using the identifiers in the nodes.

3.1.3 Canetti Krawczyk Proof Model

This model defines protocol that may run simultaneous multiple local copies of message, which is used in the system for multipath routing. Each channel can be considered as a separate session which has its own local state. Each session must have the same session identifier to communicate with each other. The purpose of each session is to establish a pair-key between the two nodes currently running.

If (Session_id(SN1,SN2)==1)
then

Communication will be established;
else
Communication terminated;

By using the same approach session is created between two nodes which need to communicate. Through this the communication becomes more secure. Multiple sessions can be created for a single node; as a result a single node can communicate with two or more nodes simultaneously. When a message is passed from one node to the other only then the session is be created after which only all key generation process will start over.

3.1.4 Security Perspective

The main perspective of SLEACH algorithm is to elect the cluster head which is a legitimate node. This is because sometimes a node which is an attacker may be elected as a cluster head. The Base Station checks for the legitimacy of the node using the Digital Signature (RSADS/DSA). During key distribution the attackers may try to attack the system in different methods. For this various solutions are provided which are as follows. For every node three random numbers have been generated which is a subset of some random value N. These three values are used for the key generation using pair wise algorithm. The final key value is hashed using the hashing algorithm SHA-1. The advantage of this process is that even when an attacker finds the random values of any node, it has to find the algorithm through which the key is generated, even if it finds the algorithm for which key generation is used it has to break the hashing function. It is very difficult to break the hashing function which takes time. By this time the random values of the node would have changed, because these values keep on changing with respect to time.

The AES algorithm is used to encrypt the key and the message, the other side of the node decrypts the message and the key using the AES algorithm. As it is very difficult to break the AES algorithm the attacker surely takes time to break the algorithm. The Canetti Krawczyk model is used for session creation; it is very secure for communication to take place in a session. This also provides a multi-path communication in which a single node can communicate with two or more nodes simultaneously. Even in this method the same Pair wise algorithm is used for key generation. For a communication to take place a session must be established. Once a session is established it is being monitored by the cluster heads. So if an attacker tries to establish a session, the session is cut down by the respective cluster heads. The Markov Chain model is used for key generation with the present state as being used as the parameter. In the work the co-ordination of a node to generate the key is used, the node's position keeps on changing because it is in mobile it is very difficult for the attacker to identify the key.

In intra-cluster communication two nodes within the same cluster communicates with each other. In inter-cluster communication the communication takes place between nodes in one cluster to the nodes in the other cluster. The communication takes place in this process, first the node in one cluster creates a session with the cluster head of the other cluster and the cluster head creates a session with the designated node or destination node. So there requires two keys to be generated since two sessions are created. From an attackers point of view it is really difficult to crack the two keys at the same time. To reduce the overhead in key generation, the system uses triple key based communication during inter-cluster communication in which the key is generated by using the identifiers in three nodes that is in communication. For an attacker it is really difficult to find the three identifiers at a particular instance as they keep changing with respect to time (combinatorial) and with respect to position (Markov Chain). Besides these techniques which is discussed above some nodes gets attacked due to external attackers like Denial of Service. As a result some nodes get internally attacked due to the external attackers. These nodes are called compromised nodes, to overcome this problem the KDD data set is used which is a predefined data set. Some of the fields are selected from the available data set which matches the constraint to prevent the internal attackers.

As mentioned before in previous chapters the key distribution is done two phases. First Randomized Combinatorial design theory is used where a set of 3 values which is a subset of X is generated for each node using which key generation takes place. Second Markov chain model is used where a set of 3 values are generated based the position of the node using which the key is generated. AES algorithm is used for encryption and decryption and moreover hashing is done which is very difficult to break. The hashing

algorithm used is SHA-1.As discussed earlier due to the external attackers there may be some unusual behaviour in some of the nodes, these are known as the compromised nodes. These nodes are monitored and detected by the cluster head of that group. This information is passed to the Base station or Police node which has the KDD dataset. This is used to detect the compromised node and prevent it. Once a session is established between two nodes the nodes are monitored by their respective cluster head. While monitoring certain rules are verified.

Step 1. check if(SLEACH(node_id)==1) then //digital signature of the node
Step 2. check if(dist(node)<400) then //distance from the cluster head
Step 3. check if(protocol, servicetype, source bytes, dest bytes, session count, host count) matches the data set
Step 4. if matches check if(attack==”Normal”) else set session(n1,n2)=0

III. RESULTS AND DISCUSSION

A Comparison is done between the various modules of the system. The detection rate and the energy of the system is analysed for various modules like ideal network, the system with SLEACH implemented, The system with key distribution implemented (RCD, RMCM and CKM), the system with session established and the system with rules defined for internal attacks (KDD). The detection rate is said to increase linearly with respect to different modules but there is a fall during RMCM due to the overhead involved in key generation and establishment in position.

For a communication to take place between the nodes, it must establish a key for communication. The table indicates the successful establishment of pair-wise key for Combinatorial and Markov chain model. The Markov chain model establishment rate is less (in certain cases) compared to Combinatorial because it involves the position to calculate the key but Markov chain model provides more security. In an inter cluster communication, established of key through pair wise method is an overhead. Hence, triple key method is used. This table indicates the successful establishment of triple key for Combinatorial and Markov chain model. The Markov chain model establishment rate is less compared to Combinatorial because it involves the position to calculate the key but Markov chain model provides more security.

The following figures provides the details of successive key generation and establishment rates.

Communication Range Type	No . of times Key Generation Functions invoked at different time intervals (KGF)	No . of times Key successfully Established at different time intervals (KSE)		
		RCD	RMCM	CKM
INTRA CLUSTER	50	35	34	45
	75	52	51	68
	90	79	76	86
INTER CLUSTER	45	35	33	44
	70	50	50	67
	85	75	75	84

Communication Range Type	Successful Pair-wise Key Establishment Rate (%) (PKER)		
	RCD	RMCM	CKM
INTRA CLUSTER	70	68	90
	69	68	91
	87	84	95
INTER CLUSTER	77	73	98
	71	71	96
	88	88	99

Communication Range Type	Average Successful Pair-wise Key Establishment Rate (APKER)			Average Successful Triple Key Establishment Rate (ATKER)		
	RCD	RMCM	CKM	RCD	RMCM	CKM
INTRA CLUSTER	75	74	92	---	---	---
INTER CLUSTER	78	77	98	77	75	93

The following measures indicate the various performances of the proposed work.

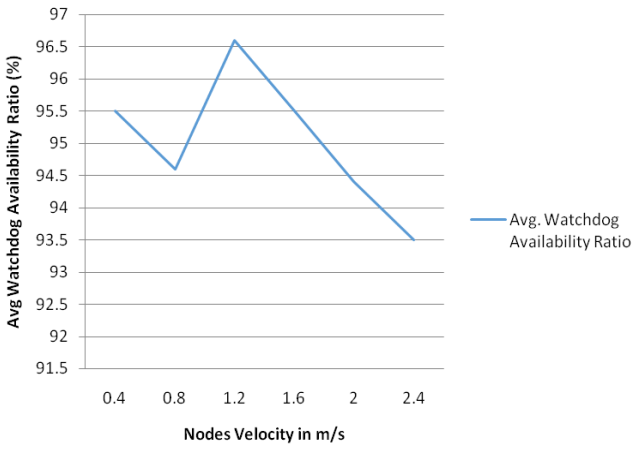


Figure 4.1 - Key generation and establishment

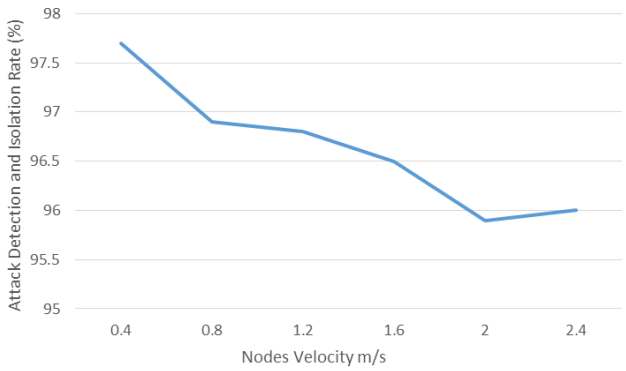
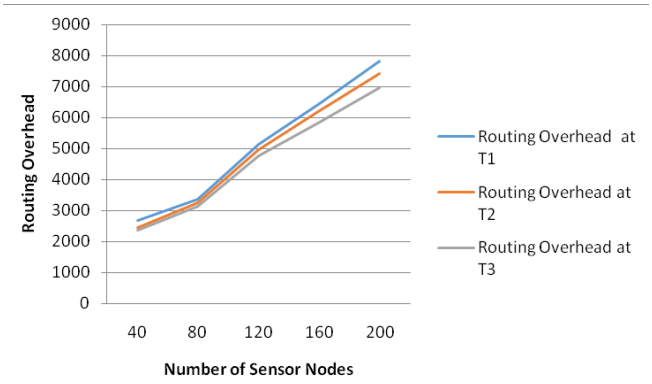


Figure 4.2 - Node velocity based performance



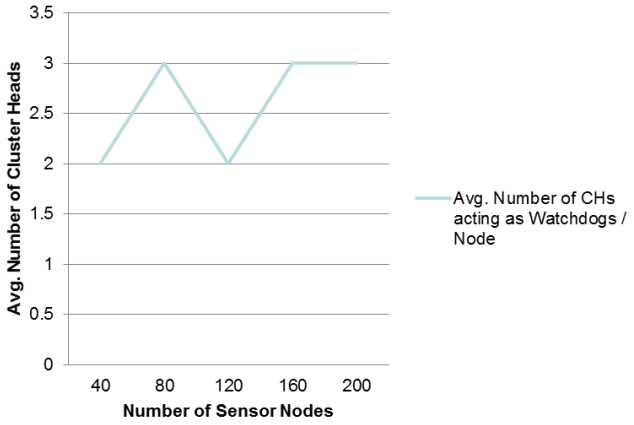


Figure 4.3 - Node population based performance

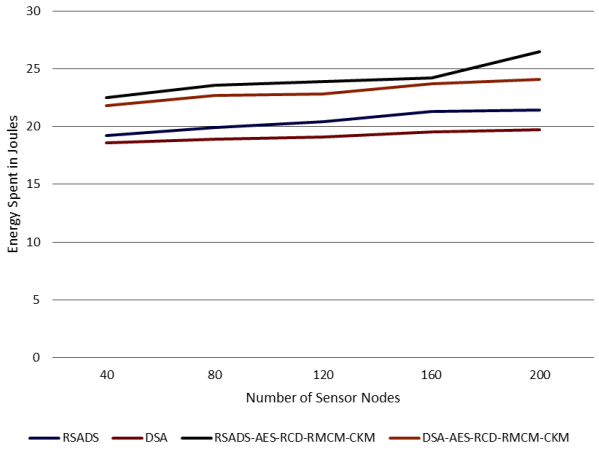


Figure 4.4 - Techniques based Energy consumption

IV. CONCLUSION AND FUTURE WORK

By using this proposed model a secured path can be established for communication. The system provides security at different point in time starting from cluster head election (SLEACH), secure data transfer through session establishment CKM with inclusion of pair wise key establishment (RCD and RMCM) in case of intra-cluster communication and triple key establishment in case of inter-cluster communication and watchdog nodes with rules definition and KDD data set. Hence, as a system it provides different layer of security and monitoring. Certain rules for internal attackers have been defined in the model. The KDD dataset have been used as a protective measure in the model. The KDD dataset can be well trained and implemented in the future so that a better secured system can be implemented. Also with respect to key distribution and establishment randomized combinatorial design theory and markov chain model has been used. RMCM is surely grant security in terms of key distribution but further improvements can be made on successful key generation rate.

V. REFERENCES

[1] Sushmita Ruj, AmiyaNayak,and Ivan Stojmenovic,"Pairwise and Triple Key Distribution in Wireless Sensor Networks with Applications", IEEE transactions on computers, vol. 62, no. 11, pp. 2224-2237 november 2013.

[2] **S. S. Kasirajan**, R. V. K. Manoj Kumar; S. B. Manoj, **S. Rajasoundaran, P. Narayanasamy**, "An analytical approach to secured routing protocol using pre-key distribution in clustered wireless sensor networks" , 2014 IEEE International Conference on Information Communication and Embedded Systems (ICICES).

[3] Walid Bechkit, Yacine Challal, Abdelmadjid Bouabdallah, and Vahid Tarokh, "A Highly Scalable Key Pre-Distribution Scheme for Wireless Sensor Networks", IEEE transactions on wireless communications, vol. 12, no. 2, pp. 948-959 february 2013.

[4] Sooyeon Shin, Taekyoung Kwon, Gil-Yong Jo, Youngman Park, and Haekyu Rhy, "An Experimental Study of Hierarchical Intrusion Detection for Wireless Industrial Sensor Networks", IEEE transactions on industrial informatics, vol. 6, no. 4, pp. 744-757 november 2010.

[5] Tingyao Jiang, Gangliang Wang and Heng Yu, "A Dynamic Intrusion Detection Scheme for Cluster-based Wireless Sensor Networks", proceedings of 2010 conference on dependable computing (cdc'2010) november 20-22, 2010, yichang, china.

[6] Hichem Sedjelmaci, Sidi Mohammed Senouci, Mohammed Feham, "Intrusion Detection Framework of Cluster-based Wireless Sensor Network ", Abou Bakr Belkaid University, STIC Lab, Tlemcen, Algeria 2012.

[7] Zhenwei Yu, Jeffrey J. P. Tsai, and Thomas Weigert, "An Automatically Tuning Intrusion Detection System", IEEE transactions on systems, man, and cybernetics—part b: cybernetics, vol. 37, no. 2, pp. 373-384 april 2007.

[8] Xin Zhou, Xiaofei Tang," Research and Implementation of RSA Algorithm for Encryption and Decryption" 2011 The 6th International Forum on Strategic Technology.

[9] Mohammad Reza Rohbanian, Mohammad Rafi Kharazmi, Alireza Keshavarz-Haddad, Manije Keshtgary, "Watchdog-SLEACH: A new method based on SLEACH protocol to Secure Clustered Wireless Sensor Networks", ACSIJ advances in computer science: an international journal, vol. 2, issue 3, no. , pp. 10-117 2013.

[10] Th. Arampatzis, J. Lygeros, and S. Manesis, "A Survey of Applications of Wireless Sensors and Wireless Sensor Networks", Proceedings of the 13th Mediterranean Conference on Control and Automation Limassol, Cyprus, June 27-29, 2005.

[11] A. Perrig, J. Stankovic, and D. Wagner., "Security in wireless sensor networks. *Commun.", ACM*, 47(6):53–57, 2004.

[12] Yvonne Hitchcock, Colin Boyd and Juan Manuel Gonz_alez Nieto, "Tripartite Key Exchange in the Canetti-Krawczyk Proof Model", Progress in Cryptology - INDOCRYPT 2004