International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 13 (2018) pp. 11324-11329

Securing Wireless Networks Using Trust Based Adaptive Acknowledgement

Ramakanth Reddy Malladi[1], Dr.A.Govardhan[2]

[1]Research Scholar, Nagarjuna University, Vijayawada, Andhra Pradesh, India.
[2]Professor of Computer Science and Engineering, JNTUH, Hyderabad, Telangana, India.

Abstract

Wireless Sensor Networks (WSN) are prone to various attacks. Different schemes have been used to reduce the malicious nodes from the network. In the environment of WSN, various schemes have used ACKs to detect routing misbehavior or malicious nodes. ACK based routing solves ambiguous collisions, receiver collisions, and will use limited transmission power. To improve security in wireless networks the best mechanism Trust. In this paper we present a Trust Based Intrusion Detection System(IDS) for Wireless Sensor Networks(WSN) based on Kalman filter to predict Trust of a given node. The proposed method resulted in improved packet delivery ratio and decreased end to end delay when compared it with MS-MAC technique which makes use of flooding based routing. We show that the proposed method is efficient.

INTRODUCTION

With miniaturization and mass production of sensor nodes, WSNs are vastly utilized for monitoring environments, military surveillance, security and medical applications. The sensors are small with restricted computational resources. Data sensed and assessed by sensor nodes are communicated via wireless channels to sinks or base stations. Unlike conventional networks, wireless sensor networks are extremely resource constrained with regard to energy, transmission range and processing capability. Hence, the design of wireless sensor networks focuses more on energy efficacy and data collection (Yick et al. 2008).

The open medium and remote distribution makes wireless sensor networks vulnerable to several assaults. For instance, malicious assaulters can obtain and compromise nodes because nodes do not have physical protection. Current data collection methods presume that network nodes are cooperative (Viani et al. 2010). Several methods are suggested for detection and alleviation of malicious nodes in wireless sensor networks (Sun et al. 2014; Rezvani et al. 2015; Yu et al. 2012; Shafiei et al. 2014 and Athmani et al. 2013). They are more susceptible than wired networks and some of the shortcomings are given below in Table 1.

Table 1: WSN Vulnerabilities

Resource availability	Security threat
Scalability	Security will be low in a dynamic network with mobility
Cooperativeness	Underlying working principle of Wireless Sensor Networks is cooperation which can likely affect the network by malicious nodes
Dynamic topology	Impacts the trust relationship among nodes
Limited power supply	Intruders can use this vulnerability to destroy the network
Bandwidth constraint	When sensor nodes are mobile, within the network it exhibits variable link quality
No predefined Boundary	Outside network communication is possible because of Networks dynamic nature

Base station locations impact network performance. For maximization of network lifetimes, it is better if base stations are nearer or amongst network nodes (Shi & Hou 2009). Centralized administration through usage of base stations improves control packet overhead and power utilization in wireless sensor networks. IDS deployed at all nodes alleviate energy utilization by nodes. IDS obtain information for diagnosing the systems security status (Sun et al. 2007). It focuses on discovering security breach or vulnerabilities leading to breaches. A typical IDS is illustrated in Figure 1.

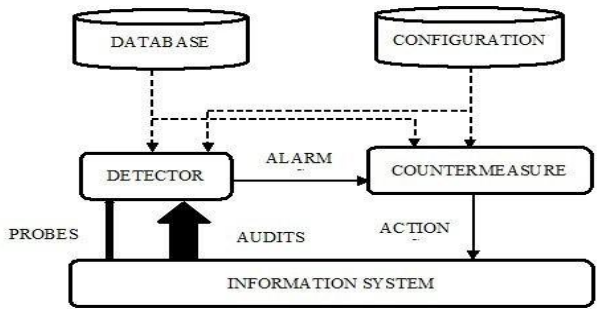

Figure 1: A simple Intrusion Detection System

IDS is a detector that utilizes three type of information (Scarfone & Mell 2007): long-term information associated with intrusion detection methods utilizing attacker knowledge bases expertise, configuration information regarding current state of the system and audit information that describes events in the system. Detectors eliminate non - required information from audit trails and present security related actions synthetic views. A decision evaluates probability that actions and/or the state can be considered intrusion symptoms or vulnerabilities. Counter measure component makes sure of corrective measures for preventing execution of actions or reverting system to secure state.

Many Schemes in wireless networks to detect routing misbehaviour or malicious nodes have used a mechanism called ACKs. The basic idea of TWOACK scheme is that whenever nodes send data packets over next hop, a special twohop ACK called TWOACK indicating that data packets were received will be send back to the next-hops destination node link (Chenguang Xuejun 2008; Liu et al 2007). Packets of TWOACK are almost similar to ACK packets either in MAC layer or TCP layer.

A node in WSN acknowledges its data packet receipt by forwarding back a two-hop TWOACK packet along active source route. In case of a TWOACK packet corresponding to a specific data packet sent out failed to be received by the data packet sender/forwarder, the next-hops forwarding route will broken and it will be declared are misbehaving node. Thus, routing protocol avoids doubtful link in future which enhances the overall network throughput performance. The Selective TWOACK scheme variant is obtained from basic TWOACK scheme, in order to decrease routing overhead due to excessive TWOACK packets (Madhavi 2008). The proposed scheme solves the problems of ambiguous collisions, receiver collisions, and limited transmission power. Nevertheless both the schemes ACK and TWOACK have high control packet overheads and may not be adequate for wireless sensor networks.

METHODOLOGY

In wireless sensor networks, maximization of battery life is crucial for enhancing the network lifetime. Almost all algorithms at data link layer attain this through following of periodic sleep/wake cycle for sensors. Already existing MAC protocols on the basis of this method are confirmed to be energy effective for static networks (Zhao 2012), however performance deteriorates in mobile networks because of delay in creation of paths. S-MAC stands for Carrier Sense Multiple Access MAC protocol with periodic coordinated sleep/wake cycles. Networks are split into virtual clusters in S-MAC and every cluster has its own sleep/wake cycles. Nodes forward and obtain information packets during wake time and information transmission follows carrier sense and RTS/CTS process (Ye et al. 2004).

In S-MAC Virtual cluster formation is based on when nodes first turn on and also random. Nodes adopt their neighbours schedule once they wake up and upon seeing various schedules, it starts functioning as border node with primary and secondary schedules. For communication within its virtual clusters one can use primary schedule and to communicate with other clusters secondary schedule can be used. Nodes broadcast their schedules for pre-determined quantity of cycles such that their neighbours may update schedules. Size of clusters continues to increase as nodes continue to wake up. Nodes are resynchronized in a periodic manner for avoiding time drift. S-MAC functions well for static networks however it is not effective within single virtual cluster. MS-MAC, a variant of S-MAC addresses sensor mobility (Pham Jha 2005). In MS-MAC, node mobility is identified on the basis of received signal strength and loss of connection which is validated after a time out period. This data is forwarded so that all nodes are made aware of their relative position with respect to the others.

In order to compute the likelihood using estimated local information we use Kalman filter. This estimation is useful in measuring the trust component in order to achieve the desired goal. Trust calculations based on Kalman is the benefit of the components being utilized along with other trust update systems. Weights may also be employed with external components and thereby providing more flexibility. Common Kalman filter process is displayed in Figure 4.2. It is noted that rather than Minimum Mean Square Error (MMSE), the local estimates are passed through time varying trust-sensitive filters (Otero et al. 2015; Somasundaram Baras 2009). From the hello message of each node of the modified routing protocol we can get normalized time varying trust values w (i; j) [n].

$$InitN[0], \hat{v}_i \quad = v(0), n = 0$$

Repeat

$$n \leftarrow n+1;$$

$$p[n] = AN[n-1]A^T + BQB^T$$

KalmanGain

$$k[n] = P[n]H_i^T (R_i + H_i p[n] H_i^T)^{-1}$$

Local Correction

$$\varsigma i[n] = A\hat{v}_i[n-1] + k[n](Z_i[n] - H_i A\hat{v}_i[n-1])$$

Exchange trust Values $\hat{u}_j \forall_j \in N + (i)$

$$\hat{u}_j[n] = \sum_{jinN+(i)} W_{ij} X \varsigma_i[n]$$

Estimation o*f* MSE

$$N[n] = (I - k[n] = H_i[n])P[n]$$

Kalman filter is a set of recursive mathematical equations presenting a way for estimating dynamic systems current state beginning from observations with arbitrary errors. For easing presentation, mono-dimensional systems with states governed by the following:

$X_t+1=X_t+V_t, t=1,2,.....$——(1)

i.e. state of system at time t + 1 relies on state of system at time t and an arbitrary process noise term Vt. Making periodic observations yt of system, such that in (2):

$y_t=X_t+W_t, t=1,2,.....$——(2)

Observations depend on current system state and an arbitrary metric noise term Wt. Individual trust lit levels, a single value Ts,t[0, 1], which denotes a nodes overall trust worthiness level is calculated through composition of utilities from individual attributes in (3):

Table 2: Simulation set up

Total Area of Network	Circulararea2kmdiameter
Maliciousness	0%,10%,20%and30%
Mobility	Random way point
Transmission range of node	100m
Radio propagation model	Free space
Traffic for simulation	Constant Bit Rate

$$T_{s,t} = \frac{\sum_{i=1}^{n} w_i * l_{it}}{\sum_{i=1}^{n} w_i} = \frac{\sum_{i=1}^{n} w_i * (1 - x_{it})}{\sum_{i=1}^{n} w_i}$$

Where wi implying weights given to service attributes. Ts,t is 0 for untrustworthy nodes, and 1 for nodes which realistically predicts services quality. Overall trust level is helpful in reputation systems for disseminating Bs reputation as Ts,t (B), where B is an intermediate node. Adaptive Acknowledgment scheme is illustrated in Figure 3. A timing-window method is resorted to node level, where trust levels are predicted. The trust values calculated in a certain time window is taken into consideration and earlier records are eliminated (Ishmanov et al. 2015)

AACK is an ACK-based network layer strategy regarded as a fusion of TACK and ACK. AACK decreases network overheads and maintains identical network throughput in comparison to TACK..

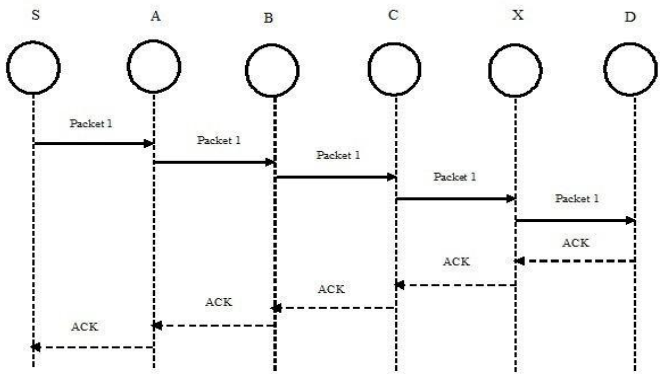

Figure 2: Adaptive Acknowledgment scheme

In AACK displayed in Figure 2 (Shakshuki et al. 2013), source S transmits packet 1 with no overheads. Intermediary nodes transmit the packet. When destination D obtains Packet 1, it forwards an ACK acknowledgment packet to source back through the same path. Within a pre-specified amount of time, if source obtains ACK acknowledgment packet, the communication of packet from source to destination is regarded a success. Otherwise, source changes to TACK and forwards a TACK packet. The concept of taking up a hybrid strategy in AACK decreases network overheads. Therefore, Trust AACK identifies malicious nodes and decreases network overheads.

In TRAACK, AACK packet is transmitted on the basis of trust condition in (4)

If nodes are extremely trustworthy across the entire route, then AACK is not transmitted. This decreases control packet overhead. In the event of medium trust, AACK is transmitted at arbitrary sequence for ensuring that packets are not disturbed along the route. If route trust is low then AACK is used. The route metrics use the trust value to select the path. The Trust Based Adaptive ACK (TRAACK) IDS proposed in this work is based on active successful deliveries where the Kalman filter predicts node trust. A Modified Acknowledgement similar to two ACK is proposed wherein entire route based trust strength is reverted to source. Based on trust value (low, medium or high) of entire route, AACK is initiated on chosen packets to decrease control overhead. Packets for which source receives AACK is based on the routes trust value. The AACK scheme is possible on any source routing protocol. This follows that AACK packets derive route from source route established for corresponding data packet.

Several methods for detecting and preventing packet dropping assaults are suggested by several authors. The methods are broadly classified as:

RESULTSANDDISCUSSION

Simulations are performed by considering MS-MAC as the MAC layer protocol, and for routing a simple flooding mechanism. The proposed TRAACK and AACK are observed for a total of five iterations. Malicious nodes were introduced in the experiment second phase. Five iterations were conducted for each scenario and the average results obtained were measured. Table 2 shows the simulation parameters used. Figures 4 to 6 and Tables 3 to 5 shows the packet delivery ratio, control packet overhead and end to end delay (seconds) respectively

QoS parameters including PDR, Routing Overheads and End to End delay are evaluated.

1) Simulation results of Proposed TRAACK for WSN.

It is observed from Table 3 and Figure 4, the packet delivery ratio of proposed TRAACK performs well at 0% malicious nodes. Also better at 20 % of malicious. For 0% malicious nodes, proposed method performs better by 2.53% than S-MAC and by 0.23% than MS-MAC. Similarly at 30%

malicious network, proposed method performs better by 65.8% than S-MAC and by 1.33% than MS-MAC

It is observed from Table 4 and Figure 5 that the control packet overhead of S-MAC is the lowest in all scenarios. For 0% malicious S-MAC performs better by 158.6% than MS-MAC and by 104% than proposed TRAACK. Similarly at 30 % malicious S-MAC performs better by 149% than MS-MAC and by 127% than proposed TRAACK. In the proposed TRAACK, based on the trust values, AACK is initiated on selected packets for decreasing control over- heads, thus it can be seen that the control overhead is lower than MS-MAC.

Table 5: End to End Delay for Proposed TRAACK

%Malicious nodes	DSR	TwoACK	Proposed TRAACK
0	0.00342	0.00386	0.00358
10	0.00418	0.00434	0.00382
20	0.00542	0.00468	0.00416
30	0.00817	0.00492	0.00434

Table 3: Packet Delivery Ratio for Proposed TRAACK

%Malicious nodes	DSR	TwoACK	Proposed TRAACK
0	0.86	0.880	0.882
10	0.76	0.860	0.860
20	0.68	0.854	0.884
30	0.42	0.821	0.832

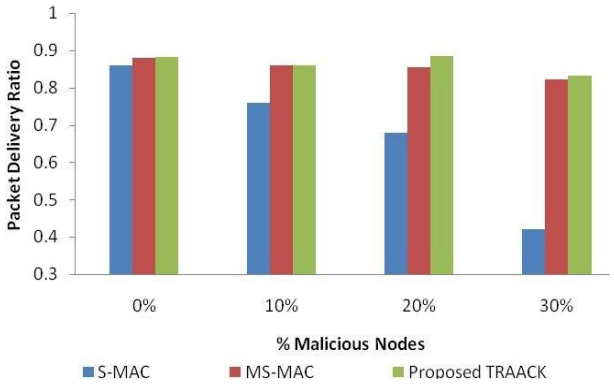

Figure 1: Packet Delivery Ratio

Table 4: Control Packet Over head for Proposed TRAACK

%Malicious nodes	DSR	TwoACK	Proposed TRAACK
0	0.030	0.260	0.095
10	0.037	0.290	0.132
20	0.042	0.302	0.186
30	0.048	0.331	0.217

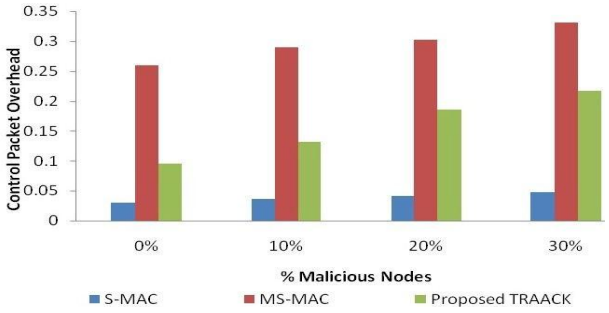

Figure 2: Packet Delivery Ratio

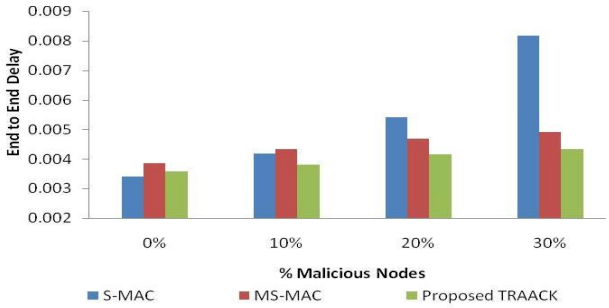

Figure 3: Control Packet Overhead

It is observed from Table 5 and Figure 6 that the end to end delay of S-MAC performs well at 0% malicious nodes. For 0% malicious S-MAC performs better by 12.09% than MS-MAC and by 4.6% than proposed TRAACK. At 30% malicious nodes, proposed TRAACK has lower end to end delay by 61.23% than S-MAC and by 12.5% than MS-MAC. Simulation results of Proposed TRAACK for MANET

Figures 7 to 9 and Tables 6 to 8 shows the packet delivery ratio, control packet overhead and end to end delay respectively. It is observed from Table 6 and Figure 7 that the packet delivery ratio of proposed TRAACK lower by 2.4% than DSR at 0% malicious and performed better by 1.2% than TwoACK. But the packet delivery ratio of proposed TRAACK performs better by 63% than DSR and by 1.24% than TwoACK at 30% malicious. It can be observed that the trust mechanism is effective only in malicious environment.

It is observed from Table 7 and Figure 8 that the control packet overhead of proposed TRAACK is higher by 161% than DSR and lower by 107% than TwoACK at 0% malicious. Similarly, the control packet overhead of proposed TRAACK is higher by 152% than DSR and lower by 131% than TwoACK at 30% malicious.

It is observed from Table 8 and Figure 9 that the end to end delay of proposed TRAACK lower by 10.8% than DSR at 0% malicious and by 6.6% than TwoACK. Similarly, the proposed TRAACK has significant lower end to end delay of 54.7% than DSR and by 12.3% than TwoACK at 30% malicious.

It is observed from Table 7 and Figure 8, the end to end delay of TwoACK is higher by 17% than DSR at 0% malicious

node. But at 30% malicious node, the end to end delay of TwoACK of delay is less by 43% than DSR. As the maliciousness increases, TwoACK performs better. The PDR for

Table 8: End to End Delay for Proposed TRAACK in MANET

%Malicious nodes	DSR	TwoACK	Proposed TRAACK
0	0.00342	0.00407	0.00381
10	0.00418	0.00455	0.004
20	0.00542	0.00499	0.00448
30	0.00817	0.00527	0.00466

Table 6: Packet Delivery Ratio for Proposed TRAACK in MANET

%Malicious nodes	DSR	TwoACK	Proposed TRAACK
0	0.86	0.83	0.84
10	0.76	0.82	0.83
20	0.68	0.84	0.85
30	0.42	0.80	0.81

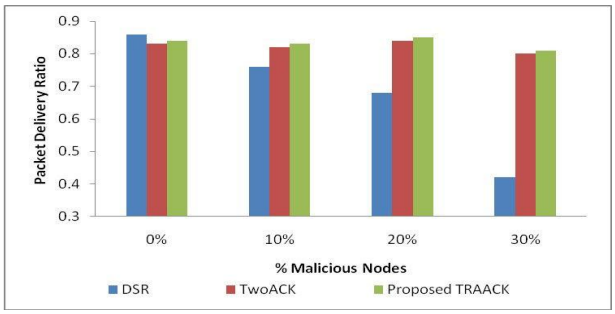

Figure 4: PacketDeliveryRatioforProposedTRAACK

Table 7: Control Packet Overhead for Proposed TRAACK in MANET

%Malicious nodes	DSR	TwoACK	Proposed TRAACK
0	0.030	0.28	0.10
10	0.037	0.31	0.14
20	0.042	0.32	0.20
30	0.048	0.35	0.23

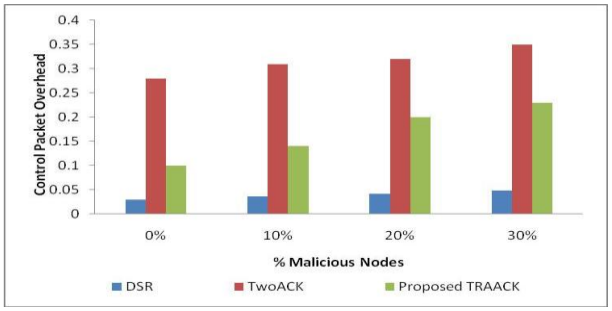

Figure 5: Control Packet Overhead for Proposed TRAACK

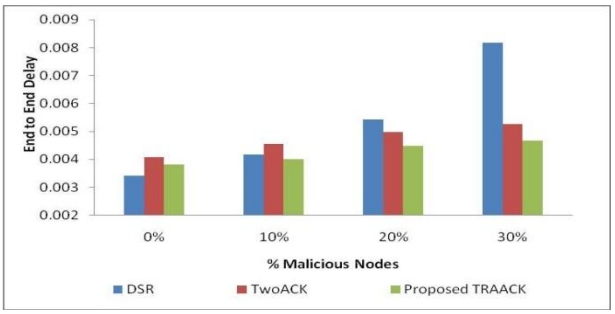

Figure 6: End to End Delay for Proposed TRAACK

DSR reduces drastically as the maliciousness in the network increases. And also, the end to end delay of DSR is higher when the maliciousness increases.

CONCLUSION

The open medium of WSN makes it vulnerable to various attacks. Various methods are incorporated to mitigate the malicious nodes from the network. ACK based routing solves ambiguous collisions, receiver collisions, and limited transmission power. To enhance wireless networks security Trust is the best mechanism. To predict node Trust an IDS mechanism for Wireless Sensor Networks is proposed in this work namely TRAACK IDS which is based on Kalman filter. A variant of Two ACK is proposed in which the entire trust strength is reverted to source. AACK is initiated on chosen route to reduce the control overhead based on trust value of the entire route. The TRAACK IDS which was proposed resulted in improved packet delivery ratio and decreased end to end delay when compared it with MS-MAC technique which makes use of flooding based routing. Further it is observed that the proposed technique exhibits improved efficiency than the AACK method as on when the maliciousness in the network gets increases. However, the control packet overheads are higher compared to MS-MAC leading to slightly higher energy consumption but yet lower than the AACK method..

REFERENCES

[1]. Yick, J, Mukherjee, B Ghosal, D 2008, Wireless sensor network survey, Computer networks, vol. 52, no. 12, pp. 2292-2330.

[2.] Viani, F, Oliveri, G, Donelli, M, Lizzi, L, Rocca, P Massa, A 2010, WSN-based solutions for security and surveillance. In Microwave Conference (EuMC), 2010 European IEEE, pp. 1762-1765.

[3]. Sun, F, Zhao, Z, Fang, Z, Du, L, Xu, Z Chen, D 2014, A Review of Attacks and Security Protocols for Wireless Sensor Networks, Journal of Networks, vol. 9, no. 5, pp. 1103-1113.

[4.] Rezvani, M, Ignjatovic, A, Bertino, E Jha, S 2015, Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks, Dependable and Secure Computing, IEEE Transactions on vol. 12, no. 1, pp. 98-110.

[5]. Yu, Y, Li, K, Zhou, W Li, P 2012, Trust mechanisms in wireless sensor networks, Attack analysis and countermeasures. Journal of Network and Computer Applications, vol. 35, no. 3, pp. 867-880

[6]. Shafiei, H, Khonsari, A, Derakhshi, H Mousavi, P 2014, Detection and mitigation of sinkhole attacks in wireless sensor networks, Journal of Computer and System Sciences, vol. 80, no. 3, pp. 644-653.

[7]. Athmani, S, Boubiche, DE Bilami, A 2013, Hierarchical energy efficient intrusion detection system for black hole attacks in WSNs, In Computer and Information Technology (WCCIT), 2013 World Congress on IEEE, pp. 1-5.

[8]. Shi, Y Hou, YT 2009, Optimal base station placement in wireless sensor networks, ACM Transactions on Sensor Networks (TOSN), vol. 5, no. 4, pp. 32.

[9]. Sun, B, Osborne, L, Xiao, Y Guizani, S 2007, Intrusion detection techniques in mobile ad hoc and wireless sensor networks, Wireless Communications, IEEE, vol. 14, no. 5, pp. 56-63.

[10]. Karen Scarfone Peter Mell 2007, Guide to intrusion detection and prevention systems (IDPS), Special Publication, pp. 800- 894.

[11]. Sun, F, Zhao, Z, Fang, Z, Du, L, Xu, Z Chen, D 2014, A Review of Attacks and Security Protocols for Wireless Sensor Networks, Journal of Networks, vol. 9, no. 5, pp. 1103-1113.

[12]. Chenguang, H Xuejun, S 2008, An energy-efficient message passing approach in MAC design for wireless sensor networks, In Circuits and Systems for Communications, 2008. ICCSC 2008. 4th IEEE International Conference on IEEE, pp. 550-554.

[13] Liu, K, Deng, J, Varshney, PK Balakrishnan, K 2007, An acknowledgment-based approach for the detection of routing misbehavior in MANETs, Mobile Computing, IEEE Transactions on, vol. 6, no. 5, pp. 536-550.

[14]. Madhavi, S 2008, An intrusion detection system in mobile adhoc networks. In Information Security and Assurance, 2008. ISA 2008. International Conference on IEEE, pp. 7-14.

[15]. Ye, W, Heidemann, J Estrin, D 2004, Medium access control with coordinated adaptive sleeping for wireless sensor networks, Networking, IEEE/ACM Transactions, vol. 12, no. 3, pp. 493-506.

[16]. Pham, H Jha, S 2005, Addressing mobility in wireless sensor media access protocol. International Journal of Distributed Sensor Networks, vol. 1, no. 2, pp. 269-280.

[17]. Somasundaram, KK Baras, JS 2009, Performance improvements in distributed estimation and fusion induced by a trusted core, In Information Fusion, 2009. FUSION'09. 12th International Conference on IEEE, pp. 1942-1949.

[18]. Ishmanov, F, Kim, SW Nam, SY 2015, A robust trust establishment scheme for wireless sensor networks, Sensors, vol. 15, no. 3, pp. 7040-7061.

[19]. Shakshuki, EM, Kang, N Sheltami, TR 2013, EAACKA Secure Intrusion-Detection System for MANETs, Industrial Electronics, IEEE Transactions on vol. 60, no. 3, pp. 1089- 1098.

[20]. Shrivastava, S Jain, S 2013, A Brief Introduction of Different type of Security Attacks found in Mobile Ad-hoc Network, International Journal of Computer Science Engineering Technology (IJCSET), vol. 4, no. 3.

[21]. Razaque, A 2015, Modular energy efficient protocols for lower layers of wireless sensor networks, (Doctoral dissertation, University of Bridgeport).

[22]. Pankaj Roha 2013, Study Analysis of Throughput, Delay and Packet Delivery Ratio in MANET for Topology Based Routing Protocols (AODV, DSR and DSDV), vol. 1, issue. II, ISSN. 2320-6802