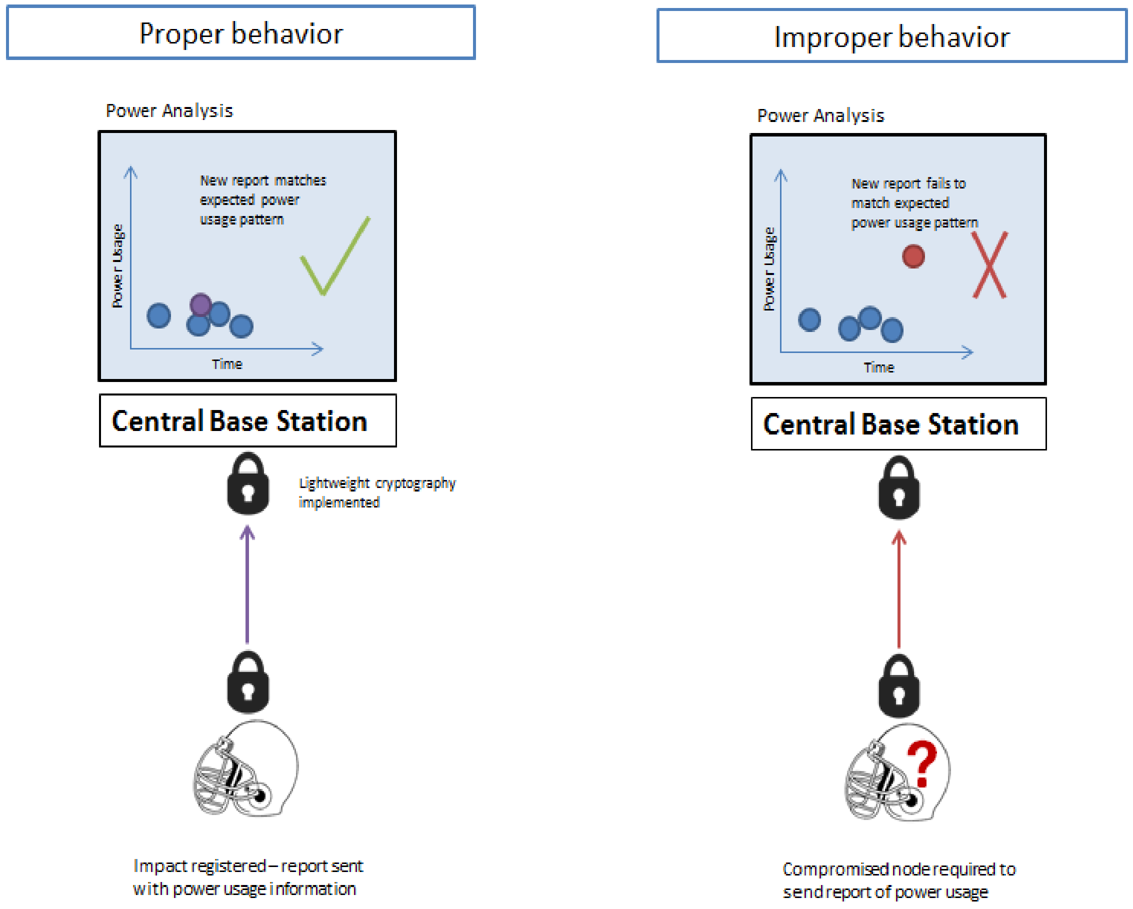
I. INTRODUCTION

Recently, professional football has been met with harsh criticism due to frequent incidents of concussions amongst players. This backlash has led to many expensive lawsuits; the NFL, in fact, recently reached a settlement of over $700 million dollars brought upon the organization due to concussions sustained by players that led to serious brain injuries [1]. To track, and eventually prevent, further injury of this type, researchers have developed football helmets that utilize wireless sensor technologies to register any occurrences of dangerous impacts that could lead to concussions.

The forerunner of such development is equipment manufacturer Riddell, a company that partnered with Simbex, a biomechanics developer, to introduce the Sideline Response System (SRS), which was first tested in 2004. This system was recently improved through the introduction of Riddell's InSite Impact Response System, a system that evolved from its SRS product. This new system uses thin polymer film to register impacts. The transmission of data in the InSite system is facilitated through the implementation of the Texas Instruments CC2530 System-on-Chip transceiver & microcontroller which utilizes a custom RF communication protocol [2]. In this way, the system forms a wireless sensor network (WSN).

WSN systems are prone to many security issues as elaborated in [3]. This is due in part to the resource-constrained nature of wireless sensor nodes, also called “motes”. Many helmet sensor systems rely on battery power; the system presented in [4], for example, implements a 3.7 V, 1800 mAh poly lithium battery. The lack of on-the-grid power requires motes to function with little processing power and highly efficient transmission of data. This resource-constrained nature, though, also leads to a greater number of security flaws. The Spy-Sense system developed in [5], for example, outlines an attack method wherein spurious transmissions are carried out by a malicious network node with healthy motes in an attempt to drain the mote of its power, eventually shutting down the network. This is a critical security flaw that affects networks such as those found in wireless helmet networks. Other attack methods, such as flooding and collision attacks, are also a concern in these low-power networks. These types of attacks may be carried out by disgruntled fans wishing to remove a player or end the game, or even terrorists hoping to disable the network for any type of malicious cause. To prevent these types of attacks on the WSN, a system on power usage reports is proposed.

alarming frequency of impacts. It is also unlikely that reports will occur with any sort of constant frequency – the sending of a report every five seconds would also be unlikely. This would fail to match accepted behavior and would therefore be registered. To assist the system in properly detecting behavior, the algorithm will be given two 'training sets', one that contains appropriate behavior and one that contains only improper behavior. The user is then notified of any anomalies, allowing for the removal or ignoring of the node.



Proper behavior
Power Analysis
New report matches expected power usage pattern
Power Usage
Time
Central Base Station
Lightweight cryptography implemented
Impact registered – report sent with power usage information
Improper behavior
Power Analysis
New report fails to match expected power usage pattern
Power Usage
Time
Central Base Station
Compromised node required to send report of power usage

Figure 1: Outline of system functioning from helmet sensor to base station

The network is composed of several helmet sensors, each with a system for monitoring and transmitting impacts as well as power reports. The sensor used is an ADXL 202, chosen for its low cost and low power usage [16]. The ADXL 202 is a 2-axis accelerometer that measures ± 2g. This module is able to send a digital signal to the microprocessor that indicates any large impacts. A hall-effect probe is also included to measure the power usage of the node. These reports may then be processed by the MCU, although only initial processing is performed by the

To ensure the confidentiality of report data, as well as its integrity and prevention against replay attacks, the AES-CCM protocol is to be implemented. This protocol consists of two algorithms – that of AES-CBC-MAC and AES-CTR to provide authentication and cipher generation, respectively. This protocol requires packets to be constructed with specific elements: a KeyId, packet number, address 2, priority octet, MAC header, and the data itself . The algorithm itself requires as input the data, a temporal key, a nonce value, and additional authentication data (AAD). This generates a new packet that contains the ciphertext as well as a message integrity code along with a nonce and AAD [17].

The AES algorithm is used multiple times through the AES-CCM process. This algorithm begins with the generation of a key schedule; the original key undergoes a one-byte circular shift which is then modified through a substitution box. This most significant byte of this operation is then XOR-ed with a round value and subsequently XOR-ed with the first column of the round key that precedes it. Round keys for subsequent rounds (10 rounds are needed for the use of 128-bit blocks) are then generated by XOR-ing the previous key's column with the previous round key. With the key schedule generated, the algorithm then encrypts through 10 rounds of modification. These rounds consist of four steps: first, each byte of the input is substituted through the use of an S-box. Then, each row of input undergoes a circular shift of a number equal to its row number (row zero does not move, row one shifts one position to the left, row two shifts two positions to the left, etc.). The next step 'mixes' the columns through taking the four bytes of each column as input and multiplying them by a polynomial (Rijndael's Galois field is used for its simplification properties). Finally, the next round key is XOR-ed with the result of column mixing to further modify each round key. This is then repeated for the indicated number of rounds – the final round, though, does not include column mixing as this is only used to further modify subsequent rounds [18].

AES-CCM, then, uses AES in the CBC-MAC protocol for authentication as follows: the temporal key is used to cipher a 128-bit block of plaintext. This is then XOR-ed with the next block of plaintext input – this result is once again ciphered with AES. This output is then XOR-ed once more with the subsequent block, and this process continues until all blocks have been processed. This results in the generation of a message integrity code.

The CTR protocol, then, operates as follows: a 128-bit counter is ciphered using AES and the temporal key – this generates the 128-bit cipherdata. The integrity code generated by the CBC-

deal of power. When a report is generated, however, it is unlikely for many others to be transmitted in rapid succession. For this reason, the motes will enter the active, more precise state upon registering power consumption that may result from an injury or abuse of the network – these reports are sent to the base station for further analysis.

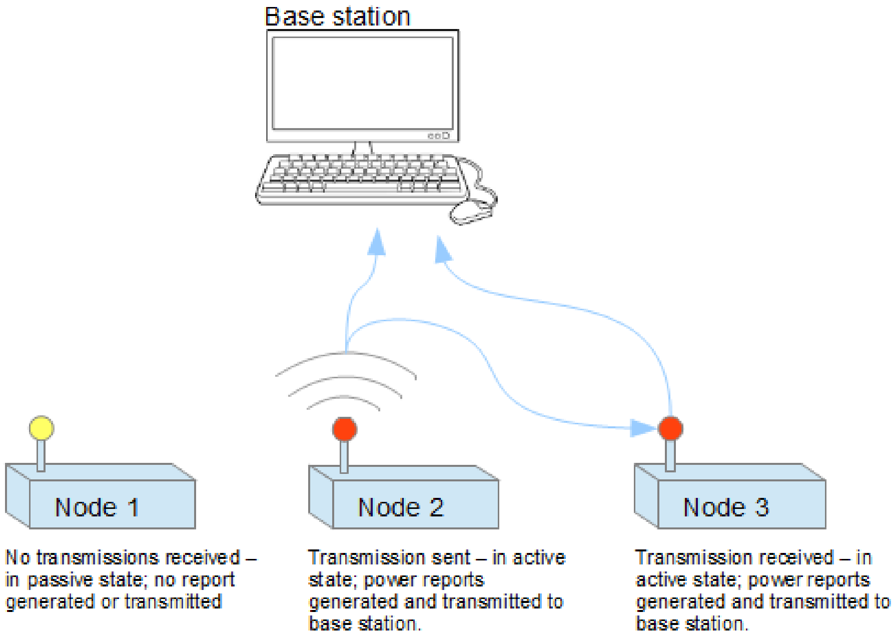

Base station
Node 1
Node 2
Node 3
No transmissions received – in passive state; no report generated or transmitted
Transmission sent – in active state; power reports generated and transmitted to base station.
Transmission received – in active state; power reports generated and transmitted to base station.

Figure 3: Functioning of active and inactive node states

IV. PROBABILISTIC MODEL

Existing methods for power analysis in security applications, such as that of Clark et al. in [6] or Hahnsang et al. In [8], utilize approaches that implement models of power usage for various application states. These power usage 'signatures' recorded during proper functioning are then compared to the functioning of the machine during questionable behavior. Classifiers, such as nearest-neighbor functions, are then used to determine whether the machine's behavior has been modified.

Keeping in mind the resource-constrained nature of helmet sensor motes, our approach is simplified. Instead of using the more complex model-based system generally used for power analysis, we propose a probabilistic model based on actual injury statistics. Using readily available statistics concerning head trauma sustained in professional football, probability

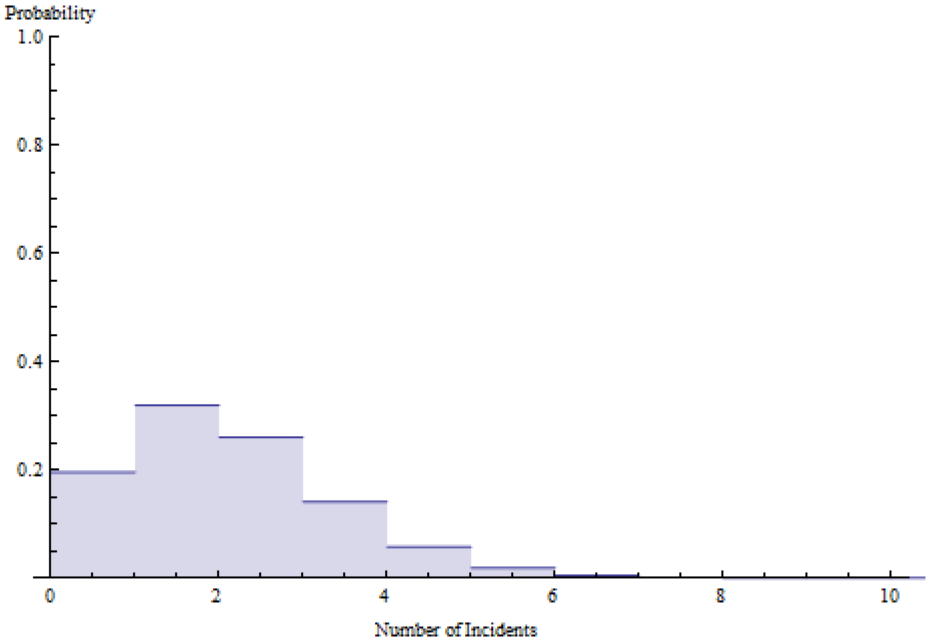


Figure 4: Example of Poisson distribution for quarterback position

To generalize this approach, a mean of the expected values may be taken, providing a value of .575. This produces a graph similar to the above, although incidents are clearly less likely:

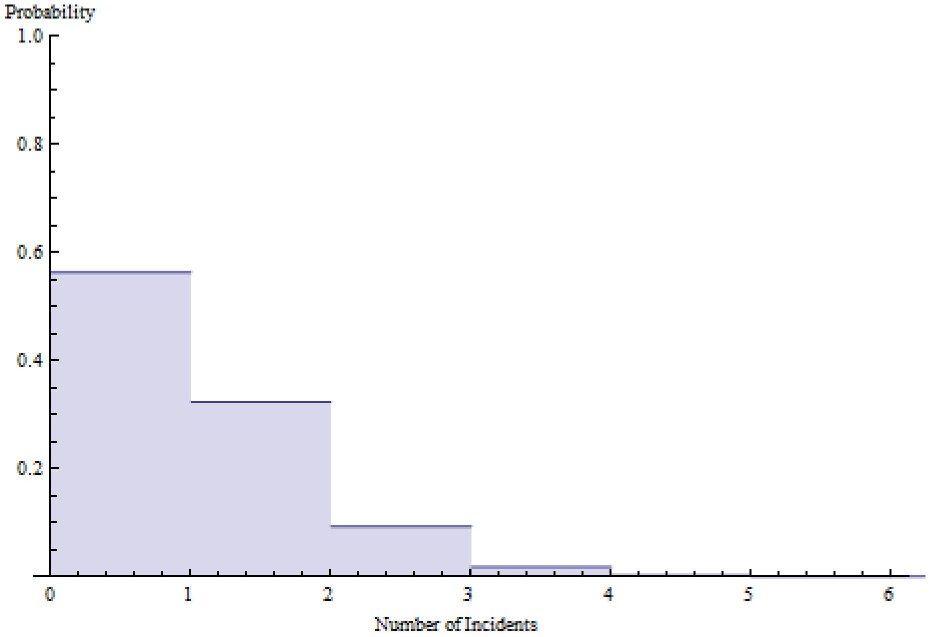


Figure 5: Poisson distribution for the generalized approach

This generalized approach may be preferred as it may be difficult to ensure players use helmets designed with their specific role in mind. This does, however, create a small loss of accuracy.

confidentiality must be maintained. The modified AES CCM mode system may prevent eavesdropping, but it cannot as easily prevent traffic analysis. While the cryptographic algorithm used may not allow the adversary to understand the reports that are generated by the application, it may still be possible for an attacker to monitor the frequency and number of reports to learn sensitive information about the network. The use of power analysis in our approach, though, prevents an attacker from using any information gained from traffic analysis as their actions must align strictly with the patterns detected in the normal function of helmet collision sensors. Any attempt at retrieving information is unlikely to align with ordinary collision patterns, thus highlighting the malicious activity.

The use of cryptography in this system may prevent against *active* attacks as well – not just passive eavesdropping. Many attacks may be carried out through unauthorized communications in the network. One such example is the neglectful and/or greedy node. A neglectful node causes damage to the network by randomly disposing of proper transmissions, thereby compromising the integrity of the network's data. Nodes may also be greedy in that they treat their own malicious transmissions as a higher priority than other nodes. This greediness allows a node to decide where traffic will flow, potentially allowing to to divert transmissions away from the base station [15]. The sinkhole attack further augments neglectful or greedy nodes as it allows them to advertise false routing information to nearby nodes. Well-behaved nodes detect the ostensibly low-latency route and take it, although in actuality it is a route through a malicious node that then drops the information [3]. This attack is particularly harmful as all nodes must then attempt to route through the black hole node, leading to heavy competition for limited bandwidth. This consumes resources and leads to breakdown of the network [15]. Another attack, that of misdirection, may be used to route the network's traffic in a similar fashion. Misdirection may be used to alter the address of many transmissions, thereby flooding the targeted node with useless message that cause its resources to be drained. In the particular application of the football helmet, it is highly important to avoid this variety of attack as the network contains a critically-important base station. If misdirection is used to route traffic away from the base station, the entire function of the network would be compromised and injuries would go unreported [15]. A variety of attack known as a HELLO flood may also be used. In this attack, malicious nodes confuse well-behaved nodes by sending HELLO packets to them despite being out of radio-range for transmission in response. This causes the nodes to believe there is a more appropriate

algorithm and ignored. Many approaches to the issue of wormhole attacks have been proposed. Hu and Evans proposed an approach that uses directional antennae for radio communication to prevent attacks [13]. This approach, however, may not be reliable for a sports-related application; a great deal of movement may require frequent calculations to determine the proper direction of the channel, leading to a greater level of overhead. This approach also requires a reliable compass to be implemented in each sensor. This may lead to a lack of reliability as the compasses in place must be able to withstand the significant impacts sustained by professional athletes.

The power analysis approach also prevents attacks that rely on the resource-constrained nature of WSN's. The aforementioned Spy-Sense system, for example, attempts to deactivate a WSN by injecting code into the heap memory of a node which then causes intensive resource usage. The algorithm used in Spy-Sense is configurable; it utilizes a custom inner loop value *IL* which wastes (.0062 * *IL*) time, on average, per cycle [5]. This wastes valuable resources, but the power analysis approach is to detect the spurious use of resources. The user would be alerted to any high levels of power usage, and the node could be inspected or deactivated without it or the entire network being destroyed. This technique is preferred over other alternatives, such as the use of mandatory access control (MAC) explained in [3]. In this approach, a protocol is put into place that limits the number of transmissions that may be made by the network's nodes, thereby preventing the excessive use of resources. Relying on protocol for this type attack prevention, though, means that there will be an increase in overhead. Any overhead increase in a WSN has a significant effect on the battery life of the system and is therefore to be avoided. Another method for the prevention of resource exhaustion is that of time division multiplexing explained in [15]. Using time division multiplexing, each node is given a specific time slot in which they are allowed to communicate. The nodes in this system, then, follow a certain order of transmission, thus preventing a malicious node from transmitting a high amount of useless data. While this may be an effective method, it leads to a waste of bandwidth. It is likely that, in the event of a sports-related impact, only a small number of helmet sensors will register a high enough force for transmission to be necessary. Assuming only one node needs to transmit following an impact, time division multiplexing would waste bandwidth until the specific range of time in which the aforementioned node may transmit is reached. In the worst-case scenario, this algorithm could waste the following amount of time:

environment, the victimized node must then allocate resources to prepare for this connection to the malicious node. Constant requests of this nature may cause the node's memory to be exhausted. While the number of connections may be limited through the hard-coding of an upper bound, this method prevents the need for such a limit as spurious connections will automatically be detected and addressed. This approach is also more efficient than another approach, that of the client puzzles mentioned in [15]. When using client puzzles, nodes on the network must first solve a “puzzle” of some kind created by the server, thus verifying that the connection is worth the solving of the puzzle and not simply spurious. Adversarial nodes, then, have a much harder time flooding a node as they must solve countless puzzles before doing so. While these puzzles may be scaled to prevent more committed adversaries, this means more latency on the network. In an application such as sports equipment which is to ensure an athlete's physical health, time is crucial and latency is to be avoided. Any increase in difficulty for the adversary is, in the client puzzle approach, and increase in difficulty for well-behaved nodes as well, and this may lead to a lower response time for emergency personnel. For this reason, the approach outlined in this paper acts to detect attempts at flooding without such a large increase of latency.

VII. IMPLEMENTATION

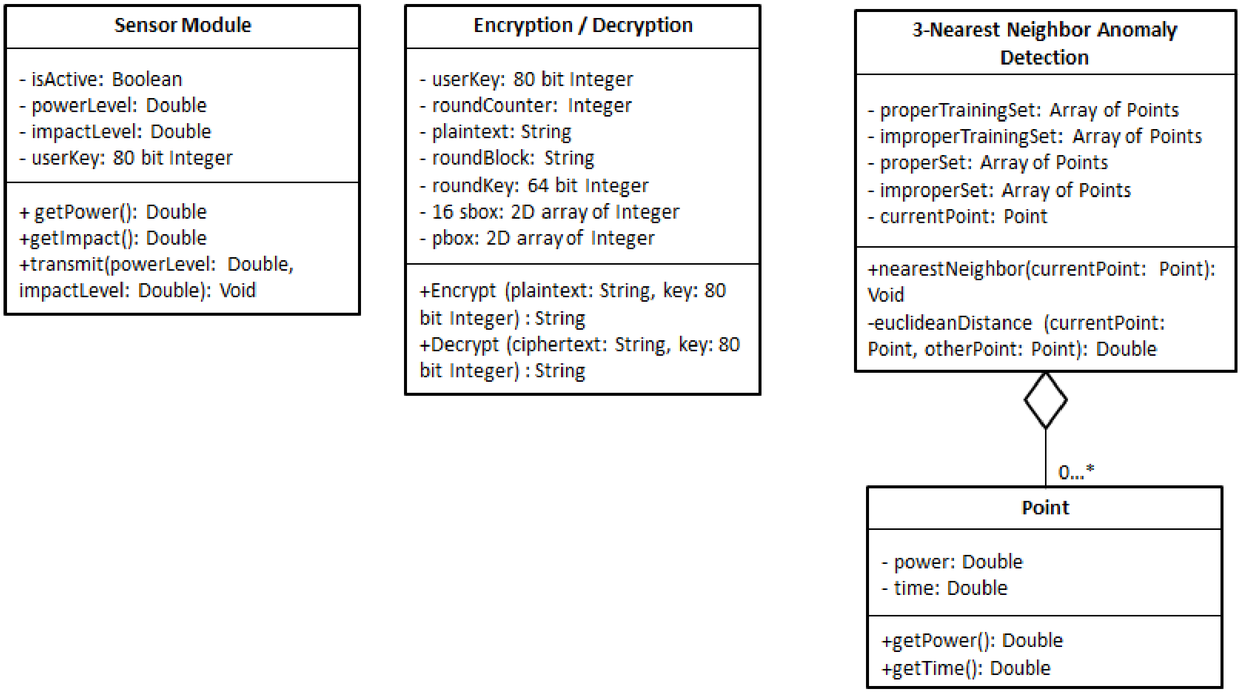

Sensor Module
- isActive: Boolean
- powerLevel: Double
- impactLevel: Double
- userKey: 80 bit Integer
+ getPower(): Double
+getImpact(): Double
+transmit(powerLevel: Double, impactLevel: Double): Void
Encryption / Decryption
- userKey: 80 bit Integer
- roundCounter: Integer
- plaintext: String
- roundBlock: String
- roundKey: 64 bit Integer
- 16 sbox: 2D array of Integer
- pbox: 2D array of Integer
+Encrypt (plaintext: String, key: 80 bit Integer) : String
+Decrypt (ciphertext: String, key: 80 bit Integer) : String
3-Nearest Neighbor Anomaly Detection
- properTrainingSet: Array of Points
- improperTrainingSet: Array of Points
- properSet: Array of Points
- improperSet: Array of Points
- currentPoint: Point
+nearestNeighbor(currentPoint: Point): Void
-euclideanDistance (currentPoint: Point, otherPoint: Point): Double
0...*
Point
- power: Double
- time: Double
+getPower(): Double
+getTime(): Double

Figure 6: Block diagram of classes involved in the system

football wherein injuries may be predicted in general but might also face aberrations due to differences in players' approaches to the game.

We showed how this system would be calculated mathematically as well as how it could be implemented using common, inexpensive sensors and hardware. We also explained the AES-CCM mode and compared out approach to multiple other approaches found in the literature to outline its advantages.

To verify the effectiveness of this approach, future work will require the simulation of a WSN using the proposed system. To achieve this simulation, a simulation program will be desired. One promising candidate is J-Sim due to the fact that it offers simulation of power consumption while several other wireless sensor network simulators do not [22]. This program may be used to reinforce the theoretical effectiveness of the proposed system.

REFERENCES

[1] News, V. (2013). NFL agrees to deal in concussion lawsuit. *Lanham: Federal Information & News Dispatch, Inc.* Retrieved from http://search.proquest.com/docview/1428838809?accountid=14584

[2] Lomberg, J. (2013, January 29). Sensor pad analyzes impacts in football helmets. *Electronic Component News.* Retrieved October 22, 2013, from http://www.ecnmag.com/articles/2013/01/sensor-pad-analyzes-impacts-football-helmets

[3] Sen, J. (2010). A survey on wireless sensor network security. *arXiv preprint* arXiv:1011.1529.

[4] Oh, S., Kumar, P.S., Kwon, H., Rai, P., Ramasamy, M., Varadan, V.K. (2013, April 9) Wireless health monitoring helmet for football players to diagnose concussion and track fatigue. *Proc. SPIE 8691, Nanosensors, Biosensors, and Info-Tech Sensors and Systems*, 869106 (April 9, 2013); doi:10.1117/12.2009719.

[5] Giannetsos, T., & Dimitriou, T. (2013, April). Spy-Sense: spyware tool for executing stealthy exploits against sensor networks. *Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privac*y (pp. 7-12). ACM.

[6] Clark, S. S., Ransford, B., Rahmati, A., Guineau, S., Sorber, J., Fu, K., Xu, W. (2013) WattsUpDoc: Power Side Channels to Nonintrusively Discover Untargeted Malware on

Embedded Medical Devices. *Proceedings of USENIX Workshop on Health Information Technologies*.

[7] Wang, Y. T., & Bagrodia, R. (2012, August). ComSen: A Detection System for Identifying Compromised Nodes in Wireless Sensor Networks. In SECURWARE 2012, The Sixth International Conference on Emerging Security Information, Systems and Technologies (pp. 148-156).

[8] Hahnsang Kim, Joshua Smith, and Kang G. Shin. (2008). Detecting energy-greedy anomalies and mobile malware variants. In Proceedings of the 6th international conference on Mobile systems, applications, and services (MobiSys '08). ACM, New York, NY, USA, 239-252. DOI=10.1145/1378600.1378627 http://doi.acm.org/10.1145/1378600.1378627

[9] Fix, E., Hodges, J. L. (1951) Discriminatory analysis, nonparametric discrimination: Consistency properties US Air Force School of Aviation Medicine, Vol. Technical Report 4, No. 3.

[10] Dudani, S. A. (1976). The distance-weighted k-nearest-neighbor rule. Systems, Man and Cybernetics, IEEE Transactions on, (4), 325-327.

[11] Engels, D., Fan, X., Gong, G., Hu, H., & Smith, E. M. (2010). Hummingbird: ultra-lightweight cryptography for resource-constrained devices. In Financial Cryptography and Data Security (pp. 3-18). Springer Berlin Heidelberg.

[12] A. Bogdanov et al. (2007). PRESENT: An Ultra-Lightweight Block Cipher. Proc. Workshop Cryptographic Hardware and Embedded Systems (CHES 07), LNCS 4727, Springer, pp. 450-466.

[13] Hu, L., & Evans, D. (2004, February). Using Directional Antennas to Prevent Wormhole Attacks. In NDSS.

[14] Banerjee, S., & Majumder, K. (2012). A Comparative Study on Wormhole Attack Prevention Schemes in Mobile Ad-Hoc Network. In Recent Trends in Computer Networks and Distributed Systems Security (pp. 372-384). Springer Berlin Heidelberg.

[15] Wood, A.D., & Stankovic, J.A. (2002). Denial of Service in Sensor Networks. IEEE Computer,Vol. 35, No. 10, pp. 54-62, 2002.

[16] Lee, Y., Kim, J., Son, M., & Lee, J. H. (2007, August). Implementation of accelerometer sensor module and fall detection monitoring system based on wireless sensor network. In

Engineering in Medicine and Biology Society, 2007. EMBS 2007. 29th Annual International Conference of the IEEE (pp. 2315-2318). IEEE.

[17] Algredo-Badillo, I., Feregrino-Uribe, C., Cumplido, R., & Morales-Sandoval, M. (2010). Efficient hardware architecture for the AES-CCM protocol of the IEEE 802.11 i standard. Computers & Electrical Engineering, 36(3), 565-577.

[18] Heron, S. (2009). Advanced encryption standard (AES). Network Security, 2009(12), 8-12. doi:10.1016/S1353-4858(10)70006-4

[19] Crisco, J. J., Wilcox, B. J., Beckwith, J. G., Chu, J. J., Duhaime, A., Rowson, S., . . . Greenwald, R. M. (2011). Head impact exposure in collegiate football players. Journal of Biomechanics, 44(15), 2673-2678. doi:10.1016/j.jbiomech.2011.08.003

[20] Ibrahim S. I. Abuhaiba, & Hubboub, H. B. (2012). Swarm flooding attack against directed diffusion in wireless sensor networks. International Journal of Computer Network and Information Security, 4(12), 18-30.

[21] Casson, I. R., Pellman, E. J., & Viano, D. C. (2008). Concussion in the national football league: An overview for neurologists. Neurologic Clinics, 26(1), 217-241. doi:10.1016/j.ncl.2007.11.005

[22] Shen, Yanfeng, and Victor Giurgiutiu. "Predictive modeling of nonlinear wave propagation for structural health monitoring with piezoelectric wafer active sensors." Journal of Intelligent Material Systems and Structures 25.4 (2014): 506-520

.