Security in Wireless Sensor Networks for Health Monitoring Helmet with Anomaly Detection using Power Analysis and Probabilistic Model

Biswajit Panja
University of Michigan-Flint
Flint, MI 48502
bpanja@umflint.edu

Zachary Scott
University of Michigan-Flint
Flint, MI 48502
zascott@umflint.edu

Priyanka Meharia
Eastern Michigan University
Ypsilanti, MI 48197
pmeharia@emich.edu

Abstract— **Litigation faced by the NFL has called for better prevention and understanding of concussions and other sports injuries. To achieve this, sports officials have turned to wireless sensor networks, or WSNs, in the form of helmet sensors that automatically report any harmful injuries to attendants on the sidelines. While this approach provides players with a greater assurance of safety and a faster response to their injuries, the security weaknesses of WSNs must be addressed. These systems, being not only recently developed but also highly resource-constrained, may be easily manipulated by those looking to gain information about players (a form of passive attack) or even attempting to remove them from the game through the sending of false reports (a form of active attack). To prevent attacks such as these, we propose a system that uses a modification of the AES-CCM protocol as well as a novel attack detection system that uses probabilistic methods to report any harmful behavior to the user. The system's power usage due to injury reports is compared to a probability model that is based on past research that recorded the likelihood of injury for the positions played in professional football. This system offers many advantages over conventional cryptography as it is a lightweight approach that costs few resources; individual helmet sensors need only send simple power reports to a central base station which uses on-the-grid power to conduct security analysis. Provided below is detail of the paper which describes the problem in greater detail, a section that details the system architecture, a section that explains the AES-CCM protocol, and an explanation of the probabilistic approach. This is followed by a security analysis that compares the approach to several other approaches found in the literature, and finally a conclusion.**

Keywords-security; wireless sensors; power analysis

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.

This system implements a combination of lightweight cryptography and machine learning to accomplish reliable security. A modification of the AES CCM mode is used to authenticate all communications and ensure data has not been compromised. Power analysis is then used to detect any intrusions that may subvert standard cryptographic methods. This system is implemented through the sending of power reports which contain information on the power usage of each node. By sending these reports with every transmission, the base station may analyze the power usage of the entire system. A 3-nearest neighbor machine learning algorithm is then used

978-1-4799-5594-7/14/$31.00 ©2014 IEEE

to detect any anomalies in the power usage reports – any attempt at draining the nodes of power resources or sending spurious reports will be detected as its activity will not match accepted behavior given to the base station before implementation.

II. ARCHITECTURE

In this section we discuss the architecture of the proposed approach. We start with analyzing proper behavior with improper behavior.

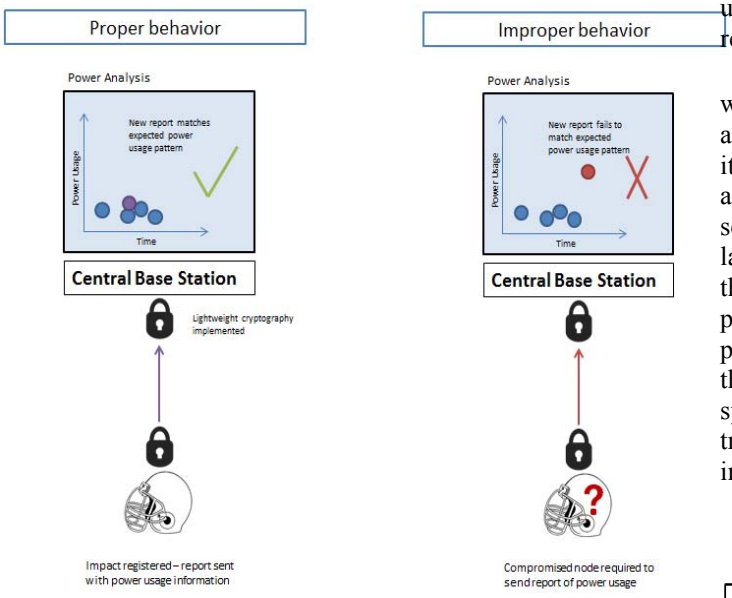

Figure 1: Outline of system functioning from helmet sensor to base station

The system consists of a network of sensors (illustrated above as a helmet sensor) described below in greater detail. These sensors make up a WSN that may be configured for a sports team such as that of professional football. The helmet sensors record impacts and send any reports of unhealthy damage to the central base station. To protect these connections, a lightweight cryptography algorithm based on the AES CCM mode is implemented. Further intrusion detection is then accomplished through the sending of additional information on each node's power usage; when any impact reports are sent, they are accompanied by a power usage report from any nodes involved in the transmission of data. This information is then compared by the base station to acceptable node behavior based on a machine learning algorithm, that of the nearest neighbor described below. When the network functions as it should, the power reports align with acceptable behavior and functioning continues. When a malicious node attempts to modify the network, though, it is highly likely that this activity will not follow the patterns of acceptable use – this anomaly is noted through abnormal power usage which is detected through the nearest neighbor algorithm. In general, helmet collisions will obey a somewhat predictable clustering; it is likely that multiple collisions will occur in a short time period. If the system detects high levels of power usage (hundreds of reports sent in five seconds, for example), it is likely that this is caused by malicious behavior as it is impossible for players to register such an 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.

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 MCU due to resource constraints. An injury threshold, measured in g's, must be hard-coded into the system. Only reports that exceed this threshold, then, will be transmitted. A similar power-usage threshold is to be implemented as well.

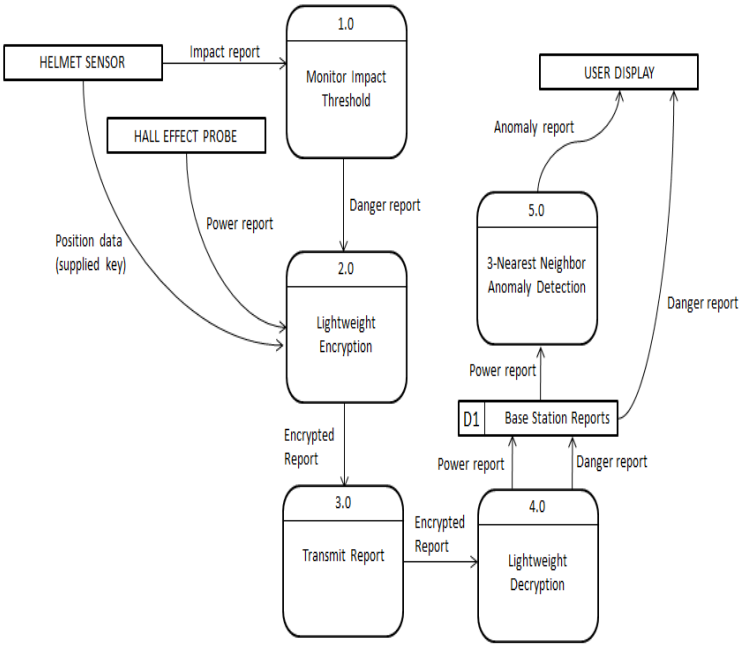

Figure 2: Data flow diagram for the proposed system

The above diagram outlines the flow of data throughout the system. Data is initially drawn from the helmet sensor. This data undergoes the process of impact threshold monitoring to determine if any serious damage has been done. If damage is detected, data flows in the form of a 'danger

report' combined with a power report constructed from data supplied by the hall effect probe. This data is then encrypted and transmitted to the base station where it is decrypted and stored. The 3-nearest neighbor power analysis algorithm is then applied to detect any anomalies. These reports, as well reports of any injuries, are then sent for user display.

III. MODIFICATION OF AES-CCM MODE

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-MAC process is then XOR-ed with the first 64-bit block of cipherdata. The counter is then incremented and ciphered again with AES and the temporal key. The integrity code is XOR-ed with the newly generated cipherdata, and this process is repeated until all data has been processed [17]. Using these two processes in sequence, then, provides authentication and encryption.

To detect any anomalies that may indicate attempts at modify the system, a system that performs power analysis similar to that of [6] is implemented. A hybrid approach, similar to that implemented in [7], is put into place to ensure the transmission is efficient. Resource-constrained motes perform basic detection of power aberrations based on preset thresholds; reports of such activity are then transmitted to the more capable base station for detailed analysis. A system such as this may detect strange behavior that is often caused by an attempt at compromising the aforementioned cryptographic approach and alert the users of the base stations so that it may be addressed effectively.

To achieve this intrusion detection, an approach may be taken such as that of [8]. Power monitoring may be achieved through the addition of a power monitoring module on each mote. The equation given in [8] to approximate power consumption is as follows:

$$V_c \Sigma\, Vi\, \Delta t$$

Where V_c represents the voltage of the lithium ion battery and V_i represents a voltage measured that is proportional to the current drawn by the battery (this is determined through the use of an oscilloscope and hall-effect probe in [8]). This work also provides a moving average to filter out any outliers in the data – this prevents many false positives. The moving average is ideal for a WSN as it is a much more energy efficient function than more sophisticated approaches.

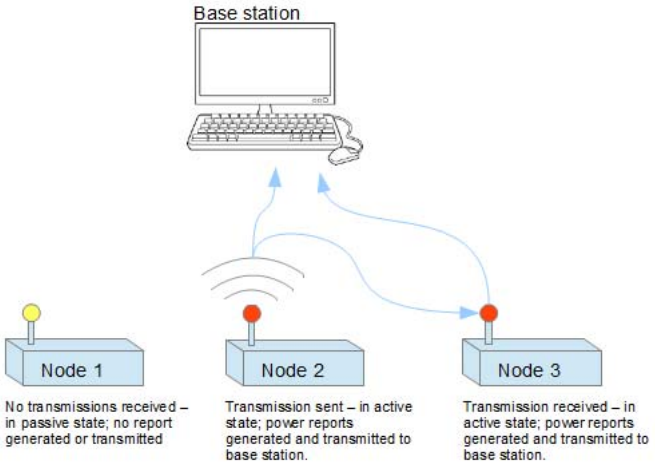

Figure 3: Functioning of active and inactive node states

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 distributions may be used to ensure that the behavior of the sensor nodes closely matches expected behavior.

The most reliable data on concussion incidences in professional football was recorded by Casson et al. In 2004 [21]. This data may be used to create a Poisson distribution in the following form:

$(e^{-\lambda}\lambda^{k})/k!$

Where e is the base of the natural logarithm, λ is the expected number of impact reports based on reported data, and k is the actual number of reports detected. The reports given in [21] are specific to the position played by each player – this allows for the creation of specific models for each player.Using this data, the probability of incidence for each position can be mapped. 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.

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. Through this probabilistic modeling approach, the power-usage behavior of the system may be analyzed as power reports should closely match these distributions – if reports contain anomalies that do not match this model, abuse of the system may have occurred.

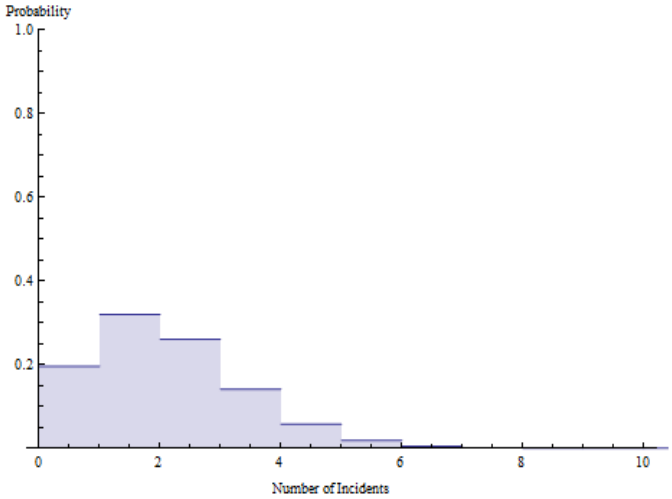

Figure 4: Example of Poisson distribution for quarterback position

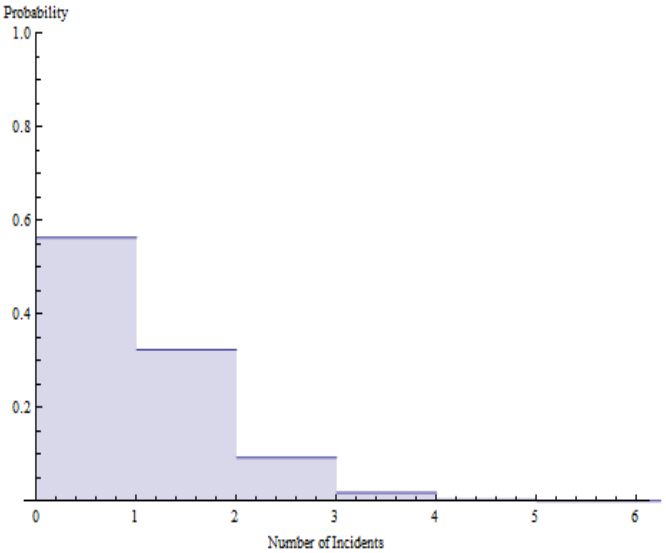

Figure 5: Poisson distribution for the generalized approach

V. Security Analysis

The lightweight cryptography implemented through the modified AES CCM mode system will allow for some security measures, the majority of which prevent the attacks on privacy illustrated in [3]. These are generally *passive* attacks, meaning that the adversary simply collects data and does not alter the functioning of the network. In an eavesdropping attack, for example, the attacker may simply record the transmissions and interpret them for their own gain. As our application deals heavily with information related to the personal health of the players, data 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 route for transmission; an attempt is made to transmit data from the node to these malicious nodes, but they are far beyond radio-range, and the data is lost [13]. While these attacks pose a great threat to WSNs, the use of lightweight cryptography in the system works to prevent these attacks that cannot be detected through power analysis alone. Cryptography is used as an authentication method in these nodes as each transmission is signed cryptographically by the well-behaved nodes to verify their identity. This prevents the above attacks, as they rely on easy and reliable transmission with nodes in the network to re-route or alter transmissions.

However, power analysis is required as some attacks may not be prevented with cryptography alone, and its use assures security in the event that the cryptographic mechanism is subverted. One specific issue that may plague WSNs is the wormhole attack. In this variety of attack, two malicious nodes are required. These two nodes are placed in different locations within the network where they are able to communicate through a reliable, high-quality connection that is outside of the WSN. This high-quality connection gives the adversarial nodes an advantage over genuine nodes – traffic sent between these malicious nodes will arrive before any legitimate communication, allowing the nodes to manipulate the network's configuration. This is done through the sending of ROUTE REQUEST messages in the case of an on-demand protocol; as this protocol favors ROUTE REQUEST messages that arrive first at a node, the high-quality connection allows malicious nodes to send spurious ROUTE REQUEST messages which will arrive first - even if the nodes are located a greater distance away. The protocol then views this route as the most efficient path, and discards all other possible routes. In this case, then, the malicious nodes are able to dictate all traffic through that particular route. This is highly dangerous, as the adversary may then modify message contents or prevent the sending of messages entirely. The approach of geographical packet leaches also suffers from drawbacks in our application as this approach depends heavily on the knowledge of the location of each sensor. The location of each helmet sensor, though, changes frequently throughout its deployment. Many other approaches, such as those depicted in [14], require overhead to be incurred on each node – they may even avoid the shortest (ostensibly the best) route in an attempt to avoid wormholes. The power analysis approach, however, requires little overhead on each node other than that needed to track power usage. All intensive calculation, then, is performed by the base station. This approach allows for the shortest route to be taken, as any malicious nodes attempting to send several ROUTE REQUEST messages will be detected through the nearest-neighbor 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:

$[(n\text{-}1)/n] * t$

Where n represents the number of nodes on the network and t indicates the length of the time frame chosen in seconds. Assuming that 11 players are on the field (as is standard), this protocol could waste 90.1% of its bandwidth in the given worst-case. By relying on the base station's processing of power reports for the prevention of spurious transmission instead of time division multiplexing or a MAC protocol, then, overhead and time may be saved.

Spy-Sense also outlines another attempt at network breakdown: unnecessary transmission. In this exploit, random portions of the node's program data are copied and used to create payloads of the maximum allowed size. These packets are transmitted over the node's RF chip, draining its battery in the process. The node is then shut down, removing it from the network [5]. This attack is prevented through power analysis as well, as any transmissions are sent along with a report that includes the level of power being consumed. This great deal of power usage would not match the patterns given to the machine learning algorithm in the supervised stage. An attack such as this, then, would be noticed before damage could take place. The base station would be notified of this strange behavior, and the issue could be addressed.

VI. CONCLUSION AND FUTURE WORK

We have shown that WSNs used in sports injury detection may be secured through the implementation of lightweight cryptography in tandem with a probabilistic power analysis approach. This novel system is particularly well-suited to WSNs as it does not require plentiful system resources and the use of power analysis prevents attacks that are known to affect WSNs, such as the spurious reports generated by a program like Spy-Sense.

The main contribution of this research is the probabilistic approach which relies on real-world data to predict the likelihood of system behavior. These probabilities are then further honed during use through the use of machine learning; acceptable behavior allows the expected levels of injuries to be re-calculated, whereas unacceptable behavior would not affect future calculations and would be discarded. For this reason, the approach is well suited to professional football wherein injuries may be predicted in general but might also face aberrations due to differences in players' approaches to the game.

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 privacy* (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